TRABAJO FINAL DE GRADO

Grado de Administración y Dirección de Empresas y Derecho

Título: Límites de la dirección empresarial en relación a los derechos digitales de los trabajadores

Autoría: Blanca Barnadas Morera

Tutoría: Fernando Barbancho Tovillas

Departamento: Laboral

Curso académico: 2018-2019

UNIVERSITAT DE BARCELONA

Facultat d'Economia i Empresa

RESUMEN

La nueva Era digital que caracteriza la actualidad (libre circulación de datos, internet y otras nuevas tecnologías, uso del *smartphone* continuamente, etc.), ha hecho necesaria la regulación del derecho fundamental a la protección de datos. El objeto del presente trabajo es analizar precisamente esta nueva Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, que regula el derecho a la protección de datos personales en el ámbito laboral, para así determinar los límites que un empresario no debe exceder en el ejercicio del control de las actividades laborales de los trabajadores con tal de proteger sus derechos digitales.

Palabras clave: LOPDGDD; derechos digitales; desconexión digital; intimidad; geolocalización; videovigilancia; convenio colectivo.

ABSTRACT

Today's new digital era (free circulation of data, internet and other new technologies, use of the smartphone continuously, etc.), has made the regulation of the fundamental right to data protection necessary. The purpose of this paper is to analyse precisely this new Organic Law 3/2018, of December 5, on the Protection of Personal Data and the Guarantee of Digital Rights, which regulates the right to protection of personal data in the work environment, in order to determine the limits that an employer should not exceed in the exercise of control of employees' activities in order to protect their digital rights.

Keywords: LOPDGDD; digital rights; digital disconnection; privacy; geolocation; video surveillance; collective agreement.

Sumario

INTRODUCCIÓN

Las Tecnologías de la Comunicación y de la Información (las TIC), han conquistado el mundo empresarial, han llegado a convertirse en un instrumento básico e imprescindible para poder desarrollar de la manera más eficiente las actividades productivas en que consisten los modelos de negocios de cada una de las empresas, pues resulta "*casi inimaginable una empresa no conectada a la red o que no disponga de equipos informáticos dadas las ventajas competitivas que ello supone*", tal y como establece GOÑI SEIN. J.L., en su artículo *Nuevas tecnologías digitales, poderes empresariales y derechos de los trabajadores: análisis desde la perspectiva del Reglamento Europeo de Protección de Datos de 2016.*

Llevando el uso de las tecnologías de la información (cámaras de videovigilancia, sistemas de geolocalización, correo electrónico, dispositivos móviles inteligentes como *smartphones* o *tabletas,* y aplicaciones que permiten el uso de redes sociales o sistemas de mensajería instantánea como *Whatsapp*) al ámbito de las relaciones laborales, es cierto que también reportan unos beneficios en cuanto al desempeño de sus obligaciones laborales (facilitan el acceso a la información, más rapidez en las comunicaciones, permiten estar interconectados y resolver con prontitud situaciones tanto personales como profesionales). Pero, en base al contenido del artículo 18 de la Constitución Española, que reconoce el derecho a la intimidad personal y el secreto de las comunicaciones, también suponen una amenaza en la medida en que registran una inmensa cantidad de datos personales del trabajador que pueden ser utilizados con finalidades distintas a las iniciales o que caigan en un estado de visibilidad permanente. Otra de las amenazas a las que se exponen es a la desaparición de la barrera que separa la vida profesional con la vida laboral, ya que estar siempre "conectado" provoca no solo el riesgo a una prolongación ilimitada de la jornada laboral, sino una sobrecarga de trabajo que puede derivar en estrés, entre otras enfermedades.

Ante esta situación, era necesaria una regulación, pues hasta ahora, con la genérica regulación existente del Estatuto de los Trabajadores, eran los propios Tribunales quienes, caso por caso y con criterios judiciales dispares, determinaban los derechos fundamentales a proteger en el uso de las nuevas tecnologías en el ámbito laboral y los límites que el control empresarial debía alcanzar para no vulnerarlos.

Con la nueva Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y Garantía de los Derechos Digitales (en adelante, LOPDGDD), tal y como se recoge en el apartado IV del preámbulo, se pretende recoger un sistema de garantía de los derechos digitales e "*impulsar políticas que hagan efectivos los derechos de la ciudadanía en Internet promoviendo la igualdad de los ciudadanos y de los grupos que se integran para hacer posible el pleno ejercicio de los derechos fundamentales en la realidad digital*".

Con carácter posterior al análisis de esta ley, objeto del presente trabajo, se tiene por finalidad determinar cuál es su correcta implementación, así como conocer el grado de aplicación en las empresas y la existencia de posibles sanciones en consecuencia de su falta de aplicación. Para ello, se emplea una metodología más bien teórica para el análisis de la situación, ya que se basa en el estudio de la legislación vigente, así como de artículos de interés al respecto, aunque se combina con el estudio de numerosas sentencias y de convenios colectivos, con tal de corroborar si ésta se ajusta a la realidad.

Respecto a lo expuesto, el trabajo se divide principalmente en dos apartados, en el primero se pretende poner en contexto al lector respecto a la situación ya mencionada de la actual Era digital, así como la evolución de las leyes que de una manera u otra han recogido la protección de derechos fundamentales digitales, hasta la LOPDGDD. En el segundo apartado, se analizan los artículos del Título X de la LOPDGDD que hacen referencia a dichos derechos fundamentales y, a su vez se divide en cinco apartados, tantos como derechos se regulan, cada uno de ellos se acompaña de la jurisprudencia correspondiente. Por último, se plantean las conclusiones extraídas y se acompaña el trabajo de un anexo compuesto por modelos de documentos, propuestos por la Agencia Española de Protección de Datos, con tal de facilitar a la empresa el carácter obligatorio de informar a los trabajadores del tratamiento de sus datos personales.

1. Antecedentes

1.1. Necesidad de regulación en el mundo digital

Según se explica en el Preámbulo de la LOPDGDD, recogiendo literalmente la justificación de la enmienda que proponía la incorporación de este nuevo Título, el Título X,

> *Internet se ha convertido en una realidad omnipresente tanto en nuestra vida personal como colectiva. Una gran parte de nuestra actividad profesional, económica y privada se desarrolla en la Red y adquiere una importancia fundamental tanto para la comunicación humana como para el desarrollo de nuestra vida en sociedad*.

La revolución digital[1], de la que estamos siendo testigos, deja un amplio abanico de posibilidades de innovar tanto en vías de colaboración y desarrollo productivo, como a su vez, en nuevas formas de control empresarial sobre el trabajo llevado a cabo por cada uno de sus empleados.

Tanto las empresas como los trabajadores cuentan con más y mejores recursos tecnológicos para el desarrollo de su trabajo, permitiendo así una flexibilización en las relaciones jurídicas derivadas de la prestación laboral que se puede apreciar desde el momento en que los empresarios permiten a sus trabajadores trabajar a distancia gracias al almacenamiento de datos en la nube o la conexión con el servidor de la empresa, el uso de dispositivos móviles, smartphones, cuentas de correo electrónico, redes sociales corporativas, etc. y, con todo ello, conseguir una más eficiente productividad laboral.

Ahora bien, tampoco se puede dejar de obviar que la implantación de las nuevas tecnologías ha permitido al empresario tener un control del entorno laboral prácticamente ilimitado. El control sobre el uso de medios tecnológicos puestos a disposición de los trabajadores se ejerce, entre muchos otros, sobre los *smartphones*, el correo electrónico, el ordenador, el uso de internet y el acceso a páginas *webs* durante la jornada laboral, sea desde la sede empresarial o desde el domicilio del trabajador. Además, también se encuentran medidas de control empresarial a través de la geolocalización, videovigilancia o sistemas de registro o *log in* mediante huella digital.

En este sentido, se ha de tener muy presente la cantidad de datos que son recabados y, posteriormente, tratados por las empresas, información que puede ser explotada con diferentes finalidades, desde la mejora de las condiciones de trabajo (como es poder trabajar desde casa, el conocido como teletrabajo, por ejemplo) hasta la mejora de las relaciones con los clientes (conseguir una relación más rápida y directa). Se trata de herramientas de uso común en gran parte de las empresas, como el correo electrónico y el acceso a internet, hasta medidas de control por medio de imágenes y sonido, medidas que implican expresamente el tratamiento de datos personales de los trabajadores.

Atendiendo a la gran cantidad de datos de los trabajadores tratados por las empresas, se plantea una cuestión fundamental en las relaciones laborales actuales y futuras, determinar

[1] LÓPEZ CARBALLO, D.; *El impacto del RGPD en el ámbito del control laboral y la era de la innovación*; Wolters Kluwer, 25 mayo 2018.

los límites de tales tratamientos, especialmente referente al control que pueda ejercer el empresario ante incumplimientos laborales de los trabajadores puesto que de éste dependerá la licitud de las medidas aplicadas como consecuencia de su utilización.

1.2. Evolución normativa

El nuevo Reglamento Europeo de Protección de Datos, Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (en adelante, RGPD)[2], elaborado con la intención de sentar las bases de una normativa de privacidad que se adecúe a la tecnología hoy presente, entró en vigor el 25 de mayo de 2016, pero no tuvo plena aplicación hasta el 25 de mayo de 2018, permitiendo así la adaptación progresiva por parte de los Estados, Administraciones Públicas y empresas, de las medidas y mejoras que el Reglamento introduce.

Concretamente, el considerando 155 y el artículo 88.1 del RGPD, hacen expresa mención a los tratamientos de datos en el ámbito laboral, estableciendo que los Estados miembros, a través de disposiciones legislativas o de convenios colectivos, podrán elaborar normas más específicas para garantizar la protección de los derechos y libertades en el ámbito laboral,

> *En particular a efectos de contratación de personal, ejecución del contrato laboral, incluido el cumplimiento de las obligaciones establecidas por la ley o por el convenio colectivo, gestión, planificación y organización del trabajo, igualdad y diversidad en el lugar de trabajo, salud y seguridad en el trabajo, protección de los bienes de empleados o clientes, así como a efectos del ejercicio y disfrute, individual o colectivo, de los derechos y prestaciones relacionados con el empleo y a efectos de la extinción de la relación laboral.*

Y, en su apartado segundo, del artículo 88, se incluye que dichas normas también deberán especificar medidas adecuadas para preservar la dignidad humana de los interesados, así como sus intereses legítimos y sus derechos fundamentales, prestando especial atención a los sistemas de supervisión en el lugar de trabajo, entre otras.

Se debe tener en cuenta que dicho Reglamento europeo no solo será de aplicación a las empresas o profesionales responsables o encargados del tratamiento de datos con domicilio social en Europa, sino que "*se amplía a empresas o profesionales con domicilio social fuera de la UE que realicen tratamiento de datos como consecuencia de su oferta de bienes o servicios destinados a ciudadanos europeos*"[3].

Centrándonos en el ámbito español, el 18 octubre 2018 el Pleno del Congreso de los Diputados aprobó el Dictamen de la Comisión de Justicia sobre el Proyecto de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales. La ley se publicó en el BOE el 6 de diciembre y entró en vigor al día siguiente. Esta nueva Ley Orgánica 3/2018, de 5 de diciembre, sustituye[4] a la hasta ahora vigente Ley 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y a su Reglamento de desarrollo (Real Decreto

---

[2] ALARCÓN CAPARRÓS, V. [Recurso electrónico]: *GDPR: ¿qué necesitas saber del nuevo Reglamento Europeo de Protección de Datos?* Blog de Signaturit, 4 de enero de 2018.

[3] ÍDEM.

[4] Disposición derogatoria única Ley 3/2018.

1720/2007, de 21 de diciembre), normativa que tuvo que ser modificada por el Real Decreto-Ley, de 27 de julio, para adaptarla al Reglamento europeo anteriormente nombrado.

Además, es de especial interés para el trabajo la disposición final decimotercera de la LOPDGDD[5], en la que deja constancia de la modificación del texto refundido de la Ley del Estatuto de los Trabajadores a través de la incorporación de un nuevo artículo 20 bis que regula los derechos de los trabajadores a la intimidad en relación con el entorno digital y a la desconexión.

> *Los trabajadores tienen derecho a la intimidad en el uso de los dispositivos digitales puestos a su disposición por el empleador, a la desconexión digital y a la intimidad frente al uso de dispositivos de videovigilancia y geolocalización en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales.*

Este nuevo artículo, poniéndolo en relación con la LOPDGDD, viene a englobar los artículos 87 a 91, del Título X sobre la garantía de los derechos digitales que se analizarán a lo largo de este trabajo.

Como se puede observar, dicho título, además de destinarse a adaptar el ordenamiento español al Reglamento europeo y completar sus disposiciones, incorpora a su objeto la importante novedad de dirigirse a "*garantizar los derechos digitales de la ciudadanía conforme al mandato establecido en el artículo 18.4 de la Constitución*"[6].

Por último, cabe hacer referencia a la Agencia Española de Protección de Datos (en adelante, AEPD)[7], una autoridad administrativa independiente a la que se le encomienda, tal como indica el artículo 47 de la LOPDGDD, la función de supervisar la aplicación de esta ley orgánica y del Reglamento europeo y, en particular, ejercer las funciones establecidas en el artículo 57 y las potestades previstas en el artículo 58 del Reglamento europeo.

Atendiendo al artículo 57 del RGPD, en el caso de España la AEPD o bien, las autoridades autonómicas de protección de datos personales, presentan la competencia de diversas funciones de las que destaca controlar la aplicación del reglamento europeo y normativas de protección de datos correspondientes, la promoción de sensibilización del público y su comprensión de los riesgos, normas, garantías y derechos en relación con el tratamiento a través de su asesoramiento gratuito, por ejemplo. También se encarga de asesorar a las instituciones y organismos sobre las medidas legislativas y administrativas relativas a la protección de los derechos y libertades de las personas físicas con respecto al tratamiento y fomentar la creación de mecanismos de certificación de la protección de datos y sellos, así como dar su aprobación. Otras de las funciones que se le atribuyen son el tratamiento de reclamaciones presentadas por un interesado o por un organismo, organización o asociación e investigar, en la medida oportuna, el motivo de la reclamación e informar al reclamante

[5] La ley tiene el carácter de Ley Orgánica, no obstante, tiene carácter de ley ordinaria para varias de sus disposiciones. Es decir, el Título IV, VII, salvo los artículos 52 y 53, tienen carácter de Ley Orgánica junto con las disposiciones adicionales segunda y decimoséptima y las disposiciones finales primera, segunda, tercera, cuarta, octava, décima y decimosexta. En cambio, el Título VIII, IX y los artículos 79, 80, 81, 82, 88, 96 y 97 del Título X, las disposiciones adicionales, transitorias y finales que no se encuentren en alguna excepción mencionada, tienen carácter de ley ordinaria.

[6] Art 1.b) LOPDGDD sobre el objeto de la ley.

[7] IBERLEY [Recurso electrónico]: *Funciones y potestades de la Agencia Española de Protección de Datos (AEPD) en el RGDO y en la LOPDGDD*. Iberley, 12 de febrero de 2019.

sobre el curso y el resultado de la investigación, así como llevar a cabo investigaciones sobre la aplicación de la LOPDGDD y hacer los seguimientos oportunos que sean de interés.

Aparte de las funciones, el artículo 58 del RGPD atribuye a la autoridad de control de cada Estado Miembro, es decir, a la AEPD, una serie de poderes que se agrupan en poderes de investigación, poderes correctivos, de autorización y consultivos. Entre estos poderes cabe destacar como poder de investigación poder ordenar al responsable y encargado del tratamiento y, en su caso, al representante del responsable o encargado que faciliten cualquier información que requiera para el desempeño de sus funciones, llevar a cabo investigaciones en forma de auditorías de protección de datos y notificarles las presuntas infracciones cometidas del RGPD, como poder correctivo la AEPD podrá sancionar a todo responsable o encargado del tratamiento con advertencias o apercibimientos o imponer multas administrativas dependiendo de la infracción, así como ordenar la rectificación o supresión de datos personales y por último, como poderes de autorización y consultivos, podrá asesorar, emitir por iniciativa propia o previa solicitud dictámenes destinados al Parlamento nacional, Gobierno u otras instituciones y organismos, así como al público sobre cualquier asunto relacionado con la protección de datos personales.

Además, como bien se ha mencionado, la RGPD permite que las leyes de cada Estado miembro prevean una ampliación de las potestades anteriormente mencionadas y, en el caso de la LOPDGDD, se encuentran en los artículos 55 y 56 que otorgan a la AEPD potestades de regulación que las disposiciones que realice llevarán el nombre de “Circulares de la AEPD” y serán obligatorias una vez publicadas en el BOE y, el artículo 56 de la misma ley le otorga a más a más, funciones relacionadas con la acción exterior en materia de protección de datos.

2. Derechos digitales de los trabajadores y límites a las facultades empresariales

Existe un conjunto de derechos fundamentales específicamente laborales (p.ej. el derecho a la huelga) que han sido regulados precisamente para desplegar sus efectos en el ámbito de las relaciones de trabajo. Sin embargo, junto a estos derechos específicos, la Constitución Española (en adelante, CE) incluye otros derechos, también calificados como fundamentales, pero que van dirigidos a la protección de todo ciudadano, independientemente de su condición laboral, los derechos inespecíficos, entre los que se encuentran el derecho al honor y a la intimidad.

En efecto, "*los derechos fundamentales no son absolutos, sino que pueden ceder ante intereses constitucionalmente relevantes como la libertad de empresa"*[8] regulada en el artículo 38 CE, en el que se reconocen una serie de facultades de organización del trabajo y control por parte del empresario a la hora de cumplir las obligaciones laborales por parte de los empleados.

Ahora bien, hay que establecer el límite a dichas facultades de organización y control por parte del empresario, aspecto recogido en el artículo 20.3 del Real Decreto Legislativo 2/2015, de 23 de octubre por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores (en adelante, LET), artículo añadido y desarrollado por la LOPDGDD. Dicho artículo queda redactado de la siguiente manera:

> *20.3. El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad y teniendo en cuenta, en su caso, la capacidad real de los trabajadores con discapacidad.*

Además, tal y como dispone el artículo 90.2 Ley 36/2011, de 10 de octubre, Reguladora de la Jurisdicción Social (en adelante, LRJS), "*no se admitirán pruebas que tuvieran su origen o que se hubieran obtenido, directa o indirectamente, mediante procedimientos que supongan violación de derechos fundamentales o libertades públicas*".

En esta misma línea, el artículo 287 Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil (en adelante, LEC), así como el artículo 11.1 LOPJ establecen que las pruebas obtenidas, directa o indirectamente violentando los derechos o libertades fundamentales no surtirán efecto. También el artículo 55.5 de la LET dispone que "*será nulo el despido que tenga por móvil alguna de las causas de discriminación prohibidas en la Constitución o en la ley, o bien se produzcan con violación de derechos fundamentales y libertades públicas del trabajador*."

Además, tal y como regula la ley, un empresario tiene el derecho a planificar de forma libre la organización de la propia empresa y lo que ello implica, es decir, vigilar y controlar el cumplimiento del trabajador de sus obligaciones y deberes laborales, así como su rendimiento y comportamiento durante su jornada laboral para determinar la línea que sigue la empresa. No obstante, bien estos derechos los puede ejercer desde el extremo de permitir al máximo

[8] ANDEYRO, L. [Recurso electrónico]: *La utilización de programas de mensajería interna para uso personal de los empleados (Comentarios a la STC 241/2012, de 17 de diciembre)*. Deloitte en colaboración con CISS, grupo Wolters Kluwer, marzo 2013. STS 119/2018, de 8 de febrero de 2018 (FJ5.3 c)) y SSTC 115/2013, de 9 de mayo de 2013 (FJ5); 70/2002, de 3 de abril (FJ10); 143/1994, de 9 de mayo de 1994 (FJ6)

la desconexión digital (como sería que los trabajadores pudieran mantener el correo electrónico con carácter personal, además de profesional, o poder no hacer uso del dispositivo móvil de la empresa fuera del horario laboral), hasta limitarla al mínimo (como sería estableciendo que el uso del correo electrónico sea exclusivamente profesional o prohibiendo el espacio personal durante la jornada laboral).

Es por ello que se debe concretar lo que un empresario puede o no puede hacer a la hora de planificar la organización empresarial, y lo que ello implica, como una protección para el trabajador. Sin embargo, a pesar de las leyes restrictivas en cuanto a la admisión de las pruebas, es la jurisprudencia del Tribunal Supremo (TS) y el Tribunal Constitucional (TC) la que se ha ido ocupando de delimitar el poder de dirección y el control del empresario regulado en el artículo 20 del ET.

En este mismo sentido, la doctrina del TC, así como las diversas sentencias del TS referentes a dicho ámbito, establecen que este tipo de medidas de intervención del empresario cuando éstas tengan como resultado la limitación de los derechos fundamentales de los empleados, deberán cumplir con una serie de requisitos. Entre los requisitos encontramos que la intervención del empresario debe ser idónea para conseguir el resultado, necesaria, proporcionada y suficientemente justificada. Además, la doctrina del TS exige que la empresa haya difundido una política de uso y control de medios para poder intervenirlos.

Respecto a los derechos digitales de los trabajadores que se encuentran regulados en los artículos 87 a 91 de la LOPDGDD, tal y como se ha mencionado anteriormente y que ahora se analizaran, encontramos: el derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral, derecho a la desconexión digital en el ámbito laboral, derechos a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo, derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral y derechos digitales en la negociación colectiva. Derechos que, de ser quebrantados, implicaría una vulneración de derechos fundamentales de los trabajadores.

2.1. Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral

Tal y como explica Carolina Blasco Jover en su artículo *Trabajdores "transparentes": la facultad fiscalizadora del empresario vs derechos fundamentales de los empleados (I)*[9], la implantación de sistemas digitales en las empresas ha tenido un fuerte impacto en las relaciones laborales. La simple utilización del ordenador de la empresa, teléfono móvil o tableta del trabajo, redes sociales o del correo electrónico, ofrecen una cantidad inmensa de datos, tanto personales como profesionales, que hacen transparente al trabajador frente al empresario y, es justo esta situación donde se puede producir un conflicto entre los poderes direccionales del empresario y los derechos fundamentales del trabajador, especialmente del derecho a la intimidad recogido en el artículo 18.1 CE, pero también del derecho al secreto de las comunicaciones que regula el artículo 18.3 CE, el derecho al honor o a la propia imagen del artículo 18.1 CE y, también de derechos fundamentales recogidos por normas internacionales como el derecho

[9] BLASCO JOVER, C.; *"Trabajadores "transparentes": la facultad fiscalitzadora del empresario vs derechos fundamentales de los empleades (I)"*; Revista Internacional y Comparada de Relaciones Laborales y Derecho del Empleo, Volumen 6, núm. 3, julio-septiembre de 2018.

a la vida privada y familiar, de su domicilio y de su correspondencia, que regulan los artículos 8 del Convenio de Roma o Convenio Europeo de Derechos Humanos (en adelante, CEDH).

El derecho a la intimidad, por sí solo, ya es un derecho autónomo reconocido por la CE como se ha mencionado, ahora bien, con la nueva LOPDGDD, se ha querido hacer una adaptación específica al derecho a la intimidad en cuanto al uso de dispositivos digitales en el ámbito laboral. Este derecho se encuentra recogido en su artículo 86, que instaura lo siguiente:

1. Los trabajadores y los empleados públicos tendrán derecho a la protección de su intimidad en el uso de los dispositivos digitales puestos a su disposición por su empleador.

2. El empleador podrá acceder a los contenidos derivados del uso de medios digitales facilitados a los trabajadores a los solos efectos de controlar el cumplimiento de las obligaciones laborales o estatutarias y de garantizar la integridad de dichos dispositivos.

3. Los empleadores deberán establecer criterios de utilización de los dispositivos digitales respetando en todo caso los estándares mínimos de protección de su intimidad de acuerdo con los usos sociales y los derechos reconocidos constitucional y legalmente. En su elaboración deberán participar los representantes de los trabajadores.

El acceso por el empleador al contenido de dispositivos digitales respecto de los que haya admitido su uso con fines privados requerirá que se especifiquen de modo preciso los usos autorizados y se establezcan garantías para preservar la intimidad de los trabajadores, tales como, en su caso, la determinación de los períodos en que los dispositivos podrán utilizarse para fines privados.

Los trabajadores deberán ser informados de los criterios de utilización a los que se refiere este apartado.

Por lo que respecta a este derecho, como se puede ver, inmediatamente introduce un límite general al disponer que la empresa podrá acceder a los contenidos derivados del uso de medios digitales facilitados a los trabajadores, pero únicamente con el objetivo de controlar el cumplimiento de las obligaciones laborales y de garantizar la integridad de dichos dispositivos.

Este límite mencionado se encuentra restringido por varios principios que la jurisprudencia ha ido imponiendo, ya que cada vez son más los casos de sanciones y despidos disciplinarios que llegan a los tribunales bajo el supuesto que el trabajador ha hecho uso de internet o el correo electrónico corporativos para fines personales. Entre las sentencias que destacan y que se procederá a analizar se encuentran sentencias del Tribunal Supremo (STS), sentencias del Tribunal Constitucional (STC) y sentencias del Tribunal Europeo de Derechos Humanos (STEDH).

En cuanto a la jurisprudencia del TS, cabe analizar la STS 26 de septiembre de 2007 y la STS 8 de marzo de 2011.

En la primera, el Tribunal resuelve sobre el uso personal del ordenador y de internet de la empresa por navegar por páginas web poco seguras y ajenas al ámbito profesional, estableciendo que, el control empresarial es compatible siempre que sea lícito y para ello, para que el empresario pueda proceder a realizar un control del uso que hacen los trabajadores de los ordenadores de la empresa, se debe notificar con carácter previo las reglas de uso de los medios de control, así como de las medidas que se adoptarán para garantizar la efectiva utilización laboral de los medios. Ahora bien, tal y como se menciona en la sentencia, dicha notificación debe ser expresa, pues no es válido entender por consentimiento tácito el hecho que el trabajador no tenga clave de acceso al ordenador de la empresa.

El TS llega a esta decisión tras definir "*el alcance de la protección de la intimidad*" y entender que debe seguir existiendo el hábito social de tolerancia con el uso personal moderado de los medios informáticos facilitados por la empresa. El Tribunal considera que la garantía de la intimidad se extiende a los archivos personales del trabajador que se encuentran en el ordenador, por lo que no comprende únicamente comunicaciones, sino también archivos personales e incluso los denominados archivos temporales, es decir, copias que se guardan automáticamente en el disco duro de los lugares visitados a través de internet, pues tales archivos pueden contener datos sensibles en orden a la intimidad e información sobre determinados aspectos de la vida privada (como sobre la ideología, orientación sexual, aficiones personales, entre otros).

La STS 8 de marzo de 2011 introduce una matización respecto a la terminante prohibición del uso personal de los medios informáticos. Considera que la prohibición total implica que deje de existir la tolerancia empresarial y que decaiga para el trabajador la expectativa razonable de intimidad que socialmente se había formado. Por lo tanto, el simple hecho de existir esta cláusula, supone que los trabajadores quedan avisados que no les ampara garantía de confidencialidad alguna, por lo que pueden estar lícitamente sometidos a vigilancia y control empresarial.

Respecto a la jurisprudencia del TC, destacan la STC 241/2012, de 17 de diciembre y la STC 170/2013, de 7 de octubre que vienen a confirmar la STS 8 de marzo de 2011.

En primer lugar, la STC de 17 de diciembre de 2012, el contenido viene a reforzar las posibilidades de control y vigilancia, por lo que favorece la posición empresarial y lo hace dictaminando que:

> *Por una parte, la posibilidad de uso común del ordenador de todos los empleados permite considerar que la información archivada en el disco duro era accesible a todos los trabajadores, sin necesidad de clave de acceso alguna. Esta disposición organizativa de uso común permite afirmar su incompatibilidad con los usos personales y reconocer que […] la pretensión de secreto carece de cobertura constitucional*.

Por otra parte,

> *No existiendo una situación de tolerancia a la instalación de programas y, por ende, al uso personal del ordenador, no podría existir una expectativa razonable de confidencialidad derivada de la utilización del programa instalado, que era de acceso totalmente abierto y además incurría en contravención de la orden empresarial*.

Y, en segundo lugar, la STC de 7 de octubre de 2013 señala que en caso que en el convenio colectivo vigente se establezca que el correo electrónico es de exclusivo uso profesional y se añadan sanciones respecto a su utilización para fines personales para que resulte legitimada la monitorización del sistema, no se requerirá información alguna sobre las reglas de uso y control de las herramientas informáticas propiedad de la empresa.

Finalmente, de la jurisprudencia que emana del TEDH, cabe mencionar la STEDH de 5 de septiembre de 2017, caso Barbulescu contra Rumania (conocida como Barbulescu II) y la STEDH de 22 de febrero de 2018, caso Libert contra Francia.

En cuanto a la doctrina acogida por el TEDH, cabe analizar en primer lugar, la sentencia del caso Barbulescu II en la que el Tribunal cambia su propio criterio establecido en la STEDH de 12 de enero 2016 (Barbulescu I).

Así, en la primera sentencia mencionada, se enjuicia la validez de un despido producido a consecuencia de un uso personal de un conocido sistema de mensajería instantánea, *Yahoo Messenger*, instalado en el ordenador de la empresa. Ante esta situación, el trabajador demandó a la empresa ante los Tribunales del país, Rumania, por considerar vulnerados sus derechos al secreto de las comunicaciones y a la intimidad. Sin embargo, el juez de instancia como el Tribunal superior e incluso con carácter posterior el TEDH, a pesar de haber realizado tal intrusión sin advertencia previa al trabajador, le negaron su amparo por considerar que la existencia de una prohibición de uso de los medios telemáticos de la empresa para fines personales, conocida por el trabajador, legitima la vigilancia empresarial. Como se puede comprobar, la decisión del TEDH va en línea de las resoluciones dictadas por el TS y TC ya analizadas.

Ahora bien, la Gran Sala del TEDH como consecuencia de la petición de reenvío del asunto por parte del demandante, dictó la nueva sentencia Barbulescu, de 5 de septiembre de 2017. La sentencia parte del presupuesto de que el trabajador no fue convenientemente informado acerca de la política de uso de los medios tecnológicos puestos a su disposición por la empresa ni de la extensión del posible control sobre ellos.

Finalmente, el Tribunal determinó que la simple existencia de una prohibición de uso de los medios telemáticos de la empresa para fines personales no debe legitimar al empresario para realizar todo tipo de control. De este modo, para que el empresario pueda llevar a cabo un control y vigilancia empresarial, según el TEDH, las autoridades nacionales deberían tener en cuenta determinados factores[10], deberían valorar si supera un test conocido como "test Barbulescu".

Dicho test consiste en los siguientes factores:

- Se debe valorar si el empresario ha informado a los trabajadores[11] y con carácter previo de las medidas de control que pueden utilizarse, de su alcance y de su puesta en práctica.
- Valorar el grado de intrusión empresarial y su extensión, ya sea temporal o material.
- También debe valorarse si la medida adoptada se considera justificada, es decir, si existe un motivo legítimo que justifique la monitorización y necesaria, es decir, no debe ser factible para su finalidad poder aplicar otras medidas menos intrusivas y más respetuosas con la vida privada del trabajador y demás derechos fundamentales.
- A su vez, las autoridades nacionales deben evaluar si el uso al que somete el empresario los datos obtenidos mediante el control, es legítimo para el objetivo que se pretende alcanzar.
- Finalmente, se debe valorar si existen suficientes garantías para el trabajador, de manera que el hecho de acceder al contenido de sus comunicaciones debe hacerse una vez el trabajador ha sido notificado.

Aplicando dichos principios generales al asunto, el TEDH consideró que le incumbía determinar si las autoridades nacionales competentes habían logrado un justo equilibrio entre los intereses divergentes en juego, el derecho al respeto de su vida privada recogido en el artículo 8 del CEDH y, por otro lado, el derecho a controlar y cumplir con las prerrogativas del

[10] STEDH, as. Barbulescu contra Rumania, de 5 de septiembre de 2017, apdo. 120, pp. 51 y 52.

[11] Ver anexo 1. Circular informativa para los trabajadores.

empresario. Todo ello con el objetivo de poder garantizar el buen funcionamiento de la empresa.

Al evaluar las medidas de control impuestas al demandante, observó que prácticamente todos los factores a valorar no pudieron ser comprobados por los órganos jurisdiccionales nacionales y, además, añadió que el acceso al contenido de las comunicaciones pudo tener lugar en cualquier momento durante el procedimiento, ya que las autoridades nacionales no determinaron en qué momento del procedimiento disciplinario el empresario tuvo acceso a dicho contenido y según el Tribunal, esta situación va en contra del principio de transparencia. A la luz de todas las consideraciones anteriores, el TEDH consideró que no se protegió correctamente el derecho del demandante al respeto de su vida privada y su correspondencia y, en consecuencia, declaró que se produjo una violación del artículo 8 del CEDH.

En el caso de Libert contra Francia, la sentencia parece entrar en contradicción con la mencionada anteriormente, el caso Barbulescu II. El TEDH entró de nuevo a valorar si la fiscalización que efectuó el empresario en el ordenador del trabajador, aunque facilitado por la empresa, vulneró el artículo 8 CEDH.

El supuesto que se plantea es el despido de un trabajador de una empresa pública de ferrocarriles[12], por almacenar en el ordenador de la empresa una serie de archivos que resultan calificados como “personales” y en los que se encontró material pornográfico y una serie de certificados falsos expedidos en favor de terceros. Hay que tener en cuenta que el registro de los archivos fue llevado a cabo en ausencia del trabajador y sin su consentimiento.

Ante esta situación, los Tribunales franceses entendieron que no se había vulnerado el derecho a la intimidad del trabajador por existir una base legal para que el empresario procediera a la intervención del ordenador. Atendiendo a la normativa interna francesa, al empresario se le concede cierto poder de control de la actividad laboral, entre otros, acceso a los ficheros que se encuentran en el ordenador de la empresa, a excepción de los que son guardados por el nombre de “privados”, a los que solo tendrá acceso previo consentimiento del trabajador o en su presencia.

El conflicto llegó al TEDH que, tras analizar los hechos, dictaminó que su juicio coincidía con las autoridades judiciales francesas y procedió a afirmar que el control efectuado por el empresario fue totalmente lícito, justificado y proporcionado por las razones expuestas anteriormente y procedió a la no apreciación de violación del artículo 8 del CEDH. Además, en la sentencia se incluyeron observaciones del TEDH adicionales respecto a las acciones del trabajador que fueron consideradas contrarias al código deontológico de la empresa, documento que contemplaba el uso profesional de los medios tecnológicos puestos a disposición de los empleados y en el cual se toleraba de manera puntual un uso personal de los mismos, código que, según el TEDH, el trabajador claramente sobrepasó (el demandante había utilizado una parte importante de la capacidad de su ordenador profesional para almacenar archivos en causa, 1.562 archivos representando un volumen de 787 MB).

[12] Empresa del sector público que puede ser considerada autoridad pública. Concretamente se trata del Sr. Libert, trabajador de la Société Nationale des Chemins de Fer (SNCF) en la que ejercía funciones de adjunto al jefe de brigada de vigilància de la región de Amiens.

Una vez analizadas varias de las sentencias de los distintos tribunales y determinados los criterios de cada uno de ellos, se analizará la STS 8 de febrero de 2018[13] dictada en casación para la unificación de doctrina y lo hace basándose en la doctrina fijada por la Sentencia de la Gran Sala del TEDH de 5 de septiembre de 2017, el caso Barbulescu II ya analizada, en relación con la posibilidad de revisar los correos electrónicos de uno de los trabajadores.

Respecto a los hechos, la empresa despidió al trabajador demandante por motivos disciplinarios como consecuencia de un incumplimiento muy grave del código ético empresarial. La empresa, tras de un hallazgo casual en una impresora de uso compartido de dos resguardos de transferencias efectuadas por un proveedor de la empresa a favor del trabajador, procedió a iniciar una investigación de los correos electrónicos que pudieran tener alguna relación con tales transferencias. Se debe tener en cuenta que dicha intrusión se limitó temporalmente y mediante palabras clave de búsqueda. Además, debe mencionarse que la empresa contaba con una política de uso de los medios informáticos que establecía tanto la prohibición personal como la posibilidad de que la empresa pudiera vigilar el cumplimiento por parte de sus trabajadores, política que cada empleado aceptaba antes de iniciar sesión en los sistemas informáticos de la empresa.

El TS, en este sentido, considera que los criterios dictados en el caso Barbulescu II y tratados anteriormente, son perfectamente compatibles con los principios de la doctrina constitucional española (las medidas adoptadas deben ser idóneas, necesarias y proporcionales). Por tanto, el TS concluyó que no se produjo ninguna vulneración de los derechos fundamentales del trabajador y ratificó la validez y vigencia de la doctrina y jurisprudencia españolas previas al caso Barbulescu II. Además, mediante esta relevante Sentencia, se ofrece una guía de actuación más precisa a las empresas a la hora de proceder a la revisión del correo electrónico de sus empleados.

También se considera de relevante importancia la sentencia del Juzgado de los Social nº2 de Palma de Mallorca, de 28 de febrero de 2018 por la que se declaró procedente el despido disciplinario a causa de la conducta y actividad en redes sociales personales de un trabajador, fuera del tiempo y lugar del trabajo, por dañar la imagen de la empresa.

La sentencia se apoyó en el quebranto de las políticas internas de la empresa donde se imponía actuar sin ofensas, ni atentados contra la dignidad de las personas cuando los trabajadores se identificasen como trabajadores de la firma y, que además fueron expresamente aceptadas por el trabajador. Asimismo, dicho quebranto fue considerado como grave por el juzgado cuando se obtuvo como prueba un grupo de opinión de internet que no solo se censuraban las palabras de su trabajador, sino que se ponía en juego la honorabilidad de la empresa, teniendo en cuenta que las redes sociales en que se publicaba eran públicas, por lo que no existía intromisión de la intimidad del trabajador alguna. Ahora bien, atendiendo al fallo de la sentencia del TSJ de Canarias con fecha de 18 de septiembre de 2018, la conducta del trabajador debe ser grave y culpable para considerar el despido como sanción proporcional y, un uso muy ocasional de las redes sociales para fines personales en horario laboral no es motivo suficiente para justificar el despido.

[13] PONCE RODRÍGUEZ, S. Y GARCÍA SÁNCHEZ, J. [Recurso electrónico]: *Control por parte de la empresa del correo electrónico del empleado*. ElDerecho.com, Laboral; 6 de abril de 2018.

2.2. Derecho a la desconexión digital en el ámbito laboral

Una de las primeras intervenciones del Estado en el conflicto entre trabajadores y empresarios fue regular con carácter de derecho la duración de la jornada de trabajo, imponiendo una jornada máxima de 8 horas, el descanso entre jornadas, régimen de permisos y el derecho a vacaciones, entre otras. Posteriormente, con la revolución tecnológica, se han ido logrando varios avances como permitir el teletrabajo que ahora varias empresas están incorporando a su modelo de trabajo y que han supuesto grandes mejoras en cuanto a la conciliación de las responsabilidades profesionales y familiares, así como una mayor eficacia y calidad del trabajo.

Sin embargo, la sobreexplotación de dichas tecnologías ha provocado la aparición de nuevos riesgos y enfermedades profesionales que no solamente tienen un alcance físico, sino psíquico. Esto es debido a que hoy en día nos encontramos prácticamente *conectados* a cualquier hora, desde los ordenadores, ya sean personales o de trabajo y también, desde nuestros dispositivos móviles, que nos permiten conocer de los sucesos familiares, de nuestras amistades, así como estar al día del mundo y de las últimas tendencias y también, nos permite estar en contacto con nuestra empresa, compañeros de la profesión, clientes, etc. en todo momento, aspecto que dificulta poder establecer un límite entre la vida personal y profesional de los trabajadores.

Con tal de remediarlo, encontrar un punto de equilibrio, surge el derecho a la desconexión digital que tiene como finalidad proteger a los trabajadores de la presión que sufren de estar conectados y a disposición de la empresa fuera de su horario laboral y evitar que éstos puedan ser recriminados por no haber estado pendientes de sus obligaciones empresariales durante dichos periodos de descanso y así combatir el estrés y la fatiga informática que ello provoca.

En España, la LOPDGDD incorpora tal derecho a la desconexión digital en su artículo 88 que pretende marcar unos límites que las empresas deben implantar para garantizar un correcto descanso entre jornadas y así alcanzar esa conciliación de la actividad laboral y la vida personal y familiar de los trabajadores. Además, como es sabido y se remarca a lo largo de este trabajo, gracias a las nuevas tecnologías, cada negocio tiene un modelo distinto de empresa y una manera particular de llevar a cabo sus obligaciones que permite cubrir todas las necesidades y deseos de la población, pero que también dificulta poder establecer unos límites generales. Es por ello que los límites antes mencionados que la nueva ley establece se tratan de la obligación de las empresas a elaborar una política interna dirigida al conjunto de los empleados, incluyendo también a los que ocupen puestos directivos.

Esta política interna debe atender a la naturaleza y objeto de la relación laboral, dando especial importancia a los supuestos de realización total o parcial del trabajo a distancia, y deberán definir las modalidades de ejercicio del derecho a la desconexión y las acciones de formación y sensibilización del personal sobre emplear un uso razonable de las herramientas tecnológicas.

Ahora bien, sería preciso matizar la forma en que se prevé regular las modalidades del ejercicio del derecho ya que existe una notable falta de claridad[14], concretamente entre el apartado segundo y tercero del artículo citado, pues el apartado segundo señala como

[14] SERRANO OLIVARES, R.; "*Los derechos digitales en el ámbito laboral: Comentario de urgencia a la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales*"; Revista IUSLabor 3/2018, Universitat Pompeu Fabra, Barcelona.

instrumento regulatorio la negociación colectiva, es decir, se pretende que se regule a través de la aprobación de un Convenio Colectivo o, en su defecto, mediante un acuerdo de empresa y, en cambio, en el apartado tercero, el legislador dictamina: "*el empleador, previa audiencia de los representantes de los trabajadores, elaborará una política interna […]*".

De lo que se interpreta que la política interna podría ser elaborada incluso con carácter unilateral ya que únicamente se exige la previa audiencia de los representantes de los trabajadores y no un deber de consulta o negociación con la representación del personal. Eso sí, de existir un convenio o acuerdo de empresa que regule las modalidades de ejercicio del derecho, dicha política interna empresarial, aun siendo aprobada con carácter unilateral, deberá respetar sus directrices.

Esta falta de coherencia expresada, según Raquel Serrano Olivares, se podría haber resuelto si el legislador español hubiera reformado a su vez el artículo 85 LET y hubiera introducido la obligación de negociar las modalidades de ejercicio del derecho a la desconexión como sucede en el ordenamiento jurídico francés y también, como se procede la elaboración de planes de igualdad en las empresas en España. De esta forma, solo en caso de que las negociaciones fracasen, siempre y cuando se hayan llevado a cabo bajo el principio del deber de negociar de buena fe, el empresario podría hacer uso de su poder direccional y elaborar una política interna sobre el derecho a la desconexión digital de forma unilateral.

Si nos adentramos más en la parte práctica, analizando la jurisprudencia[15] existente en dicha materia, se puede ver que años atrás ya era un tema de interés. Así lo refleja la Sentencia de la Sala de lo Social de la Audiencia Nacional del 17 de julio del 1997, el Tribunal el cual declaró nulas las instrucciones establecidas por una empresa, que obligaban a mantener una conexión ininterrumpida y en todo momento de sus teléfonos móviles con los de la empresa y los de todos sus clientes una vez concluida la jornada de trabajo, debido a que consideró que dichas medidas sobrepasaban las facultades regulares de la empresa.

Otras sentencias de interés son las que se pronuncian sobre el tiempo de trabajo y la disponibilidad tecnológica como son la STJUE del 5 de octubre de 2004 (C-397/2001), asunto Pfeiffer y otros, en la que se declaró la incompatibilidad con el derecho de la UE de una norma nacional que permitía mediante acuerdo colectivo que se pudiera superar el máximo de la jornada semanal con la adición de periodos de disponibilidad, aunque se asumiera que éstos no siempre eran trabajo efectivo, sino que incluían tiempos en los que no existía actividad laboral alguna.

También la STJUE del 9 de septiembre de 2003 (C-151/2002) asunto Jaeger, que consideró periodo de descanso aquel periodo que el trabajador no estaba sujeto a ninguna obligación vis a vis con su empresario, sin impedirle el dedicarse libremente y sin interrupción a la consecución de sus propios intereses.

Cabe mencionar también la STJUE 10 de septiembre de 2015 (C-266/14)[16] por la que se estableció que el tiempo de desplazamiento entre el domicilio de los trabajadores y los centros del primer y último cliente se deben considerar como tiempo de trabajo por carecer

[15] MORENO GONZÁLEZ-ALLER, I. [Recurso electrónico]: *El derecho de los trabajadores a la desconexión tecnológica*, ElDerecho.com, Social. 17 de agosto de 2018.

[16] Caso Federación de Servicios Privados del sindicato Comisiones Obreras contra Tyco Integrated Security, S.L. y Tyco Integrated Fire & Security Corporation Services, S.A., empresa dedicada a la instalación y mantenimiento de sistemes de intrusión y sistemes antihuro en comercios en la mayor parte de las provincias españolas.

de la posibilidad de disponer libremente de su tiempo y dedicarse a sus asuntos personales. Para dictar el fallo, el TJUE, principalmente se basó en el apartado primero del artículo 2 de la Directiva 2003/88/CE que define el concepto de tiempo de trabajo como "*todo periodo durante el cual el trabajador permanezca en el trabajo, a disposición del empresario y en el ejercicio de su actividad o sus funciones*".

De modo que, de conformidad con las legislaciones o prácticas nacionales, se presume que, durante tales desplazamientos, están a disposición de sus empresarios y en ejercicio de su actividad o de sus funciones, pues este concepto se contrapone al periodo de descanso al excluirse mutuamente ambos conceptos. Esta presunción también abarca a los trabajadores que no tienen un centro de trabajo fijo durante sus desplazamientos hacia o desde un cliente. No obstante lo establecido, la Directiva 2003/88/CE no menciona la retribución de los trabajadores, únicamente se limita a regular algunos aspectos de la ordenación del tiempo de trabajo. Por lo que, para conocer de la retribución, se debe atender al Convenio Colectivo correspondiente.

Y, la más actual, la STJUE 21 de febrero de 2018 (C-518/15), asunto Matzak, que declaró que los Estados miembros no se les está permitido adoptar definiciones alternativas al concepto de tiempo de trabajo con carácter menos restrictivo que el que contiene el apartado primero del artículo 2 de la Directiva 2003/88/CE. Por lo que se interpreta, junto a lo mencionado en las anteriores sentencias, que el tiempo de guardia que un trabajador pasa en su domicilio con la obligación de responder a las convocatorias de su empresario en un plazo de ocho minutos, debe considerarse tiempo de trabajo debido a que restringe considerablemente la posibilidad de realizar otras actividades.

De aquí se extrae que cuando el tiempo de disponibilidad se dedica a una actividad relacionada con el trabajo, su naturaleza es laboral con independencia del lugar en que se preste, es decir, ya se esté realizando sus obligaciones profesionales dentro del centro de trabajo como fuera y que la interrupción con fines profesionales que entorpezca el descanso del trabajador podría ser considerado trabajo efectivo. Además, cabría en este apartado, nombrar el nuevo Real Decreto-ley 8/2019, de 8 de marzo, de medidas urgentes de protección social y de lucha contra la precariedad laboral en la jornada de trabajo, por la que se obliga a las empresas a registrar las horas de la jornada laboral de sus trabajadores[17] ya que, a pesar de que no tenga el fin de controlar la desconexión laboral, sino el abuso de horas extra y la temporalidad, indirectamente favorece en este aspecto, pues, como dice Santiago Zamora en su artículo publicado en Diario La Ley "*Dexconexión digital ¿novedad o anécdota?*", debido a la generalidad de los términos en los que se ha publicado la LOPDGDD, existe el riesgo de

> *[…] quedar en papel mojado si no van acompañadas de un desarrollo normativo que concrete las medidas específicas que deben implementar las empresas, así como un sistema efectivo de control del tiempo de trabajo que permita examinar con rigor el tiempo de trabajo empleado desde distintos medios electrónicos*[18].

Por lo tanto, gracias al registro de las horas que realiza el trabajador, tanto éste como el empresario, conocerán la jornada laboral real, es decir, las horas que el trabajador debe estar disponible para la empresa y, finalizadas éstas, tendrá derecho a desconectar el teléfono móvil o a no responder a las llamadas o mensajes con fines profesionales, ya sean a través del móvil o del correo electrónico, y sin posibilidad de imponerle sanción alguna.

[17] Ver anexo 2. Consentimiento para el tratamiento de datos biométricos.

[18] ZAMORA, S.; "*Desconexión digital ¿novedad o anécdota?*"; Diario La Ley, nº 9363, 21 de febrero de 2019.

2.3. Derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo

De acuerdo con el precitado artículo 89 de la LOPDGDD, la licitud de la utilización de los sistemas de videovigilancia para el ejercicio de las funciones de control laboral vendrá determinada principalmente por su finalidad, debiendo ser ésta la de verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales siempre que se respeten los derechos fundamentales tales como la dignidad, así como la propia imagen y la intimidad, atendiendo al artículo 20.3 ET sobre el poder direccional del empresario al que se remite.

Por lo tanto, en cuanto a las medidas de videovigilancia adoptadas, éstas se considerarán adecuadas y no excesivas, por regla general, mientras no menoscaben los derechos de los trabajadores. Sin embargo, las sentencias en unificación de doctrina, tanto del Tribunal Constitucional como del Tribunal Supremo y, ahora con la entrada en vigor de la LOPDGDD, se exige que, a pesar de cumplir con el requisito finalista, igualmente el empresario debe cumplir con el deber de informar a los trabajadores con carácter previo a la instalación de los medios de vigilancia para que dicho control sea lícito y, por ende, conservar las grabaciones como medios de prueba.

Por lo que respecta a la obligación de informar previamente a los trabajadores, la Agencia Española de Protección de Datos, a través de su Instrucción 1/2006, de 8 de noviembre, estableció en su artículo 3 apartado a), la obligación de colocar como mínimo un distintivo informativo que debe ser ubicado en un lugar suficientemente visible, ya sea en espacios abiertos como cerrados. Dicha Instrucción se redactó de conformidad con el artículo 5.1 la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal, Ley ya derogada por la disposición derogatoria única de la LOPDGDD y, es en el artículo 22.4 de la nueva ley, donde se prevén dichas disposiciones respecto al tratamiento de datos recabados a través de la videovigilancia.

> *El deber de información previsto en el artículo 12 del Reglamento (UE) 2016/679 se entenderá cumplido mediante la colocación de un dispositivo informativo en lugar suficientemente visible, identificando, al menos, la existencia del tratamiento, identidad del responsable y la posibilidad de ejercitar los derechos previstos en los artículos 15 a 22 del Reglamento (UE) 2016/679*.

Según señalaba el Tribunal Supremo en esa línea jurisprudencial, el deber de información que se debe proporcionar debe ser

> *[…] información previa y expresa, precisa, clara e inequívoca a los trabajadores de la finalidad laboral a que esa captación podría ser dirigida. Una información que debía concretar las características y el alcance del tratamiento de datos que iba a realizarse, esto es, en qué casos las grabaciones podían ser examinadas, durante cuánto tiempo y con qué propósitos, explicitando muy particularmente que podían utilizarse para la imposición de sanciones disciplinarias por incumplimientos del contrato de trabajo*[19].

Estas aclaraciones jurisprudenciales, vienen a ser confirmadas por el artículo 89.1 de la LOPDGDD.

[19] STS, de 13 de mayo de 2014 conforme a la STC 29/2013 de 11 de febrero de 2013.

Sin embargo, dicha línea jurisprudencial ha ido cambiando, en la medida que se han ido introduciendo ciertos matices y excepciones a dicha regla. Concretamente, en cuanto a la aparición de sospechas de comisión de delitos por parte de los trabajadores.

A efectos de exponer y explicar tales cambios, es básico el análisis de la Sentencia dictada por el Juzgado de lo Social, número 3 de Pamplona, de fecha 18 de febrero de 2019, en el procedimiento de despido número 875/2018, por ser la primera[20] sentencia dictada en España sobre los requisitos para la validez como prueba de las grabaciones de videovigilancia en el control empresarial, alegando e interpretando el Reglamento Europeo de Protección de Datos y la nueva LOPDGDD. Aunque, debido a la perspectiva temporal, la sentencia no pudo ser motivada con los artículos de la ley, sino en otras sentencias.

El supuesto de hecho enjuiciado en la mencionada sentencia, consistía en la instalación de una cámara de videovigilancia en una empresa[21] con el fin de vigilar las instalaciones o bienes de la misma. La empresa demandada tenía otras cámaras de vigilancia instaladas en su centro de trabajo con el correspondiente cartel identificativo de zona videovigilada. No obstante, la cámara en cuestión por la que es demandada la empresa, no fue objeto de información a los trabajadores, además de que grabó hechos que habían ocurrido fuera del centro de trabajo y de la jornada y que sirvieron para motivar la sanción muy grave de despido disciplinario del demandante (una pelea con otro trabajador).

Como se ha mencionado anteriormente, para poder llegar al fallo de la resolución, el magistrado recoge los hitos de la evolución de la jurisprudencia sobre el control empresarial mediante la videovigilancia y la incidencia del Reglamento Europeo de Protección de Datos. Entre estas sentencias, incluye la STC 98/2000, de 10 de abril (RTC 2000, 98), la STC 39/2016, de 3 de marzo (RTC 2016, 39) y la STEDH de 9 de enero de 2018.

La STC 98/2000, de 10 de abril, resolvió el supuesto de la utilización, en un casino, de micrófonos en determinadas dependencias del centro de trabajo donde eran grabadas las conversaciones de los trabajadores. La sentencia estimó el recurso y reconoció la vulneración del derecho a la intimidad personal del trabajador recurrente, sin admitir el amparo en las facultades de vigilancia y control del empresario reconocidas en el artículo 20.3 ET, debido a no cumplir con una serie de requisitos, entre los que destaca el principio de proporcionalidad e intervención mínima que posteriormente regirá otras sentencias. Dicho principio se basa en que

> *Las limitaciones […] de los derechos fundamentales del trabajador tienen que ser las indispensables y estrictamente necesarias para satisfacer un interés empresarial merecedor de tutela y protección, de manera que si existen otras posibilidades de satisfacer dicho interés menos agresivas y afectantes del derecho en cuestión, habrá que emplear estas últimas*.

El TC consideró que el casino no había cumplido con este principio porque el uso del sistema de grabación de sonido era continuado e indiscriminado de todo tipo de conversaciones, incluidos los ajenos al interés empresarial, por lo que rebasaba ampliamente las facultades

[20] LEGAL TODAY [Recurso electrónico]: *Primera sentencia sobre validez como prueba de la videovigilancia de los trabajadores tras aprobarse la LOPD.* 8 de marzo de 2019.
[21] Empresa Nucap Europe, S.L.

del empresario otorgadas por el artículo 20.3 ET y suponía una intromisión ilegítima en el derecho a la intimidad recogido en el artículo 18.1 CE.

Este principio de proporcionalidad, en contraposición, sí que se cumplía la STC 186/2000, de 10 de julio, donde el hecho enjuiciado era un despido disciplinario a causa de la sustracción de dinero de una de las cajas probado a través de unas grabaciones del sistema de videovigilancia que instaló la propia empresa para comprobar sus sospechas al respecto. Dicho principio se consideró aplicable, ya que, tras unas sospechas fundadas, la empresa procedió a la instalación de un circuito cerrado de televisión que únicamente enfocaba las cajas registradoras, con un radio de alcance máximo a las manos y, por un período de tiempo determinado. El TC, en este caso, consideró que el principio era respetado y la empresa estaba haciendo uso legítimo de su derecho a adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento del trabajador de sus obligaciones laborales (art.20.3 ET).

Por lo que el TC, en esta sentencia, reiteró el principio de proporcionalidad, lo redefinió incluyendo el cumplimiento de nuevos requisitos esenciales para que se considere una medida proporcional y pueda volver a adoptarse. Por lo tanto, se considerará una negativa a la lesión del derecho a la intimidad y a la propia imagen consagrados en el artículo 18.1 CE, siempre y cuando la medida sea justificada. Es decir, la empresa que las adopte lo debería hacer previas sospechas razonables de la comisión de irregularidades por parte de los trabajadores, además, debe ser idónea en cuanto a la finalidad que se pretende que cumpla como la de verificar tales sospechas. Y también, debe ser una medida necesaria y a su vez equilibrada, en el sentido que tales grabaciones no pueden abarcar genéricamente el cumplimiento de los trabajadores con carácter prolongado en el tiempo, sino que debe ser adoptado por un período de tiempo determinado y debe grabar únicamente el ámbito físico estrictamente imprescindible. El cumplimiento de todas estas condiciones es lo que se conoce como el cumplimiento del test de proporcionalidad[22].

Por lo referente al deber informativo, la sentencia del JS de Pamplona recoge lo establecido en la STC 39/2016, de 3 de marzo. En este caso, el supuesto de hecho resuelto por el TC parte de la instalación de una cámara de videovigilancia en un establecimiento comercial de una empresa de ropa[23], ante las sospechas de que en una de sus tiendas se estaban produciendo numerosas irregularidades contables en la caja y, con tal de averiguar y confirmar tales sospechas razonables, se procedió a la instalación de la cámara sin una previa comunicación a los trabajadores, si bien en el escaparate del establecimiento, en lugar visible, se colocó un distintivo informativo correspondiente con el artículo 3 de la Instrucción 1/2006.

Una vez evidenciado el incumplimiento laboral de la demandante, se procedió a su despido disciplinario, aportando como evidencia las imágenes captadas por el sistema de videovigilancia. Tras la comunicación del despido, la trabajadora presentó una demanda impugnando el despido y solicitaba que éste fuese declarado nulo a causa de la vulneración

[22] SJS Pamplona 52/2019, de 18 de febrero 2019, que reitera la doctrina clásica desarrollada en las SSTC 66/1995, de 8 de mayo (FJ 5); 55/1996, de 28 de marzo (FFJJ 6, 7, 8 y 9); 207/1996, de 16 de diciembre (FJ 4 e)) y 37/1998, de 17 de febrero (FJ 8).

[23] Bershka BSK España, S.A.

de su derecho al honor, intimidad y dignidad. El TC, basándose en los artículos 18.1 y 18.4 de la CE, finalmente consideró que

> *[…] no puede subsumirse el supuesto de hecho en el ámbito que protege el artículo 18.4 CE en cuanto que no se trata de la instalación de sistemas aptos para la recopilación sistemática y general de datos de carácter personal, y por eso no puede pretenderse que se diera conocimiento al trabajador vigilado*.

Por un lado, el deber de dar conocimiento al trabajador en cuestión, de información previa, debe ser exigido en función de los derechos y bienes constitucionales en conflicto, como son, el derecho a la protección de datos del trabajador en contraposición del poder de dirección empresarial imprescindible para la buena marcha de la organización productiva.

Por lo tanto, tal y como se interpreta en la SJS Pamplona de 18 de febrero de 2019, se considerará vulnerado el derecho fundamental a la protección de datos a causa del incumplimiento del deber de información previa, una vez el tribunal haya ponderado la proporcionalidad de la medida adoptada[24].

Debe quedar claro que el deber de información sigue existiendo, por lo que, aunque no sea necesario el consentimiento expreso del trabajador para el tratamiento del material obtenido a través de cámaras de videovigilancia con finalidad de seguridad o control laboral, ya que se ampara en el artículo 20.3 ET, éste se seguirá exigiendo de acuerdo con la normativa de protección de datos, que establece que es suficiente para su cumplimiento la mera exposición en un lugar visible del cartel distintivo[25] (STS 31 de enero 2017 (RJ 2017/1429), STS 1 de febrero de 2017 (RJ 2017/1105), STS 2 de febrero de 2017 (RJ 1628/2017)). Es decir, el empresario no requerirá el consentimiento expreso del trabajador para el tratamiento de imágenes obtenidas a través de cámaras instaladas por la empresa, siempre y cuando se hayan instalado por razones de seguridad, para realizar un control laboral sobre sospechas de la comisión de hechos ilícitos por empleados (como hurtos, robos, manipulación de bienes propiedad de la empresa, entre otros). Y esto es así, ya que sería absurdo exigir a la empresa que obtuviera el consentimiento de los trabajadores que se encuentran bajo sospecha de la comisión de un hecho ilícito.

Ahora bien, el empresario sí requerirá la obtención del consentimiento expreso de los trabajadores afectados cuando la finalidad del tratamiento de datos no guarde relación directa con el mantenimiento, desarrollo o control de la relación contractual, es decir, cuando el tratamiento de datos se utilice con finalidad ajena al cumplimiento del contrato.

De lo que se extrae de la STC 39/2016 es que, para ser admitidos como prueba los datos obtenidos de la instalación de cámaras de videovigilancia, éstas deben cumplir con la finalidad que recoge el artículo 20.3 ET, así como los artículos 33 y 38 CE. En estos casos, el deber de información previa ya no requiere que sea una información específica, es decir, una información previa y expresa, precisa, clara e inequívoca de la finalidad de control a la que podía destinarse los datos personales (como por ejemplo sancionar a los trabajadores), sino que este deber se subsana con otorgar a los trabajadores una información general, es decir,

[24] Debe ser una medida justificada, idónea, necesaria y equilibrada, condiciones que deben considerarse a la hora de determinar el cumplimiento del principio de proporcionalidad y que, a su vez, permitirá descartar que se haya producido lesión alguna del derecho a la intimidad personal consagrado en el artículo 18.1 CE.

[25] Ver anexo 3. Distintivo informativo de aviso de videovigilancia.

basta con la exposición en un lugar perfectamente visible de un distintivo informativo, sin ser necesaria la explicación de la finalidad concreta de la instalación de tal sistema informático.

Además del deber de información, otra de las razones necesarias que también se menciona en la STC 39/2016 para motivar la legitimación de la instalación de cámaras por parte de la empresa es que dichas medidas adoptadas cumplían el test de proporcionalidad ya que la cámara se encontraba situada en una zona concreta de trabajo, donde se desarrollaba la prestación laboral de la que se sospechaba, la zona de las cajas, y no se instaló en zonas de paso o comunes.

En cuanto a los sistemas de videovigilancia oculta o secreta, cabe destacar como sentencia más reciente, la dictada por el TEDH del caso López Ribalda y otras contra España, de 9 de enero de 2018.

El supuesto de hecho de la STEDH es el despido de varias trabajadoras de un establecimiento propio de una cadena de supermercados por la sustracción de productos de la empresa justificado por imágenes captadas por las cámaras de videovigilancia instaladas. Se trata de un caso de doble vigilancia ya que, algunas de las cámaras eran visibles y se cumplió con el deber de información previa a los representantes de los trabajadores y a los mismos empleados, así como con su finalidad, la de controlar posibles hurtos por parte de los clientes; mientras que otras se instalaron de cara a controlar directamente a los trabajadores que prestaban servicios en las cajas de los supermercados, pero de forma oculta y sin información previa de su existencia ya que se pretendía grabar los posibles robos de los empleados debido a un descuadre entre las ventas diarias y el inventario en el año 2009.

El litigio finalmente llega ante el TEDH bajo la alegación de la vulneración del artículo 8 del CEDH sobre el derecho a la vida privada y el TEDH resuelve a favor de las recurrentes motivando su fallo, principalmente, por considerar que la vigilancia encubierta se había efectuado de forma totalmente indiscriminada. En primer lugar, porque el TEDH parte de la base que la videovigilancia encubierta de un empleado en su lugar de trabajo supone una "*importante intromisión en su vida privada*", ya que el trabajador no puede evitar la grabación al estar obligado por contrato a desempeñar su trabajo en dicho lugar y, además, por el hecho de que el trabajador, debido a la falta de información, "*se ve privado de saber si le están grabando y qué se hace con esas imágenes, perdiendo todo poder de control y disposición sobre sus propios datos*".

Otro de los argumentos esenciales a tener en cuenta por la empresa, y que aplicó el TEDH, es si la medida era justificada tras ponderar los derechos que entran en conflicto. En el supuesto de hecho no se admitió, por cuanto la grabación de cámaras de videovigilancia se hizo de manera prolongada en el tiempo y a pesar de existir una sospecha, ésta no era lo suficiente razonable, ya que las cámaras no iban dirigidas específicamente a algunos empleados, sino a "*la totalidad del personal que trabajaba en las cajas, con una duración de semanas, sin límite de tiempo y durante todo el horario laboral".*

Finalmente, el TEDH consideró que los derechos de los empleados podrían haber sido más protegidos, por lo que la medida tampoco se consideró idónea, ya que se podría haber hecho uso de otros medios, concretamente informando, incluso de modo general, sobre la instalación de un sistema de videovigilancia.

Por lo tanto, no existe justificación[26] de la utilización de un sistema oculto de videovigilancia para la captación de incumplimientos laborales, al menos en el caso español no es admitida por la normativa, ya que ésta exige que, como mínimo, se coloque en un lugar suficientemente visible un distintivo informativo que incluya una referencia a la ley de protección de datos, una mención a la finalidad para la que se tratan los datos "zona videovigilada" y una mención expresa a la identificación del responsable ante quien puedan ejercitarse los derechos a los que se refiere la ley (derecho al acceso, rectificación, supresión, limitación del tratamiento, portabilidad y oposición de los datos correspondientes a cada individuo)[27], simplemente se requiere una información general, por lo que no afectaría a entorpecer la investigación de verificación de las sospechas.

Conforme a lo expresado, se pueden recoger unos parámetros generales en materia de videovigilancia:

En primer lugar, se debe poner de relieve la importancia de evaluar la medida empresarial de vigilancia a través del juicio de proporcionalidad[28]. Es decir, que la medida sea:

- Justificada (motivar por parte del empresario las sospechas fundadas respecto a la comisión de un acto ilícito de forma individualizada o bien en relación con un puesto de trabajo en concreto en el que pueden trabajar varios trabajadores).
- Idónea (en el sentido que la medida cumpla con la finalidad de evitar o prevenir, así como verificar las posibles irregularidades).
- Necesaria (por no existir otra medida menos gravosa para la consecución del propósito con la misma eficacia).
- Equilibrada (hace referencia a la ubicación de la cámara, ésta debe enfocar directamente al puesto de trabajo del que se sospeche que se están cometiendo las irregularidades y, este requisito incluye que la duración de las grabaciones deben ser breves y eliminarse todas aquellas imágenes que incluyan otros empleados o situaciones irrelevantes para la investigación).

En segundo lugar, a pesar de que el legislador español con la antigua ley[29] dejaba entrever que el cumplimiento del principio de proporcionalidad era suficiente para la validez del valor probatorio[30], con la nueva LOPDGDD, junto con la jurisprudencia del TEDH, se extrae que es de obligado cumplimiento para que se considere válida como prueba, haber informado como mínimo con un distintivo informativo en un lugar suficientemente visible.

[26] SJS Pamplona Segundo fundamento de derecho, E) 5: *Efectivamente, dado que existe un deber de informar previamente al trabajador de la instalación de las cámaras de vigilancia, ya no serán posibles y quedan absolutamente prohibidas las grabaciones encubiertas u ocultas, que es tanto decir como no informadas. Las sospechas de irregularidades graves en el desempeño de la actividad laboral no legitiman una excepción del deber de informar de la grabación que afecta al puesto objeto de sospecha, ni exonera de cumplir las exigencias del RGPD*.

[27] Artículos 13 a 18 de la Ley 3/2018, de 5 de diciembre de 2018.

[28] STEDH, as. López Ribalda y otros contra España, de 9 de enero de 2018; STS 21/2019, de 15 de enero 2019; STSJCAT 24/2019, de 8 de enero.

[29] Artículo 22.5 Ley 15/1999 de Protección de Datos de Carácter Personal, de 13 de diciembre.

[30] También así lo interpretó la STC 186/2000, de 10 de julio o la STS de 9 de febrero de 2015, que consideró admisible subsanar el deber de información previa con la información de las medidas adoptadas al presidente del comité de empresa si se consideraba que el hecho de exponer carteles informativos frustraría la investigación.

En este sentido, en caso de que el trabajador del que se sospecha sea representante de los trabajadores, sería válida la prueba obtenida sin avisar a los trabajadores ni representantes, siendo suficiente el distintivo. Ahora bien, debe constar[31] el responsable del tratamiento de los datos que se puedan extraer, así como una información a los trabajadores (que podría establecerse en el convenio colectivo) que dichas pruebas pueden derivar en sanciones disciplinarias.

Además, debe tenerse en cuenta que, tal y como se ha mencionado anteriormente, substituir la información a los trabajadores por el distintivo informativo en un lugar visible en la empresa, solo se admitirá si cumple con la finalidad de control empresarial, no si es ajeno a éste. Así lo confirma la Sentencia del Tribunal Superior de Justicia de Cataluña (STSJCAT) 24/2019, de 8 de enero (RS 6190/2018) cuando establece en su tercer fundamento de derecho:

> *El trabajador conocía que en la empresa se había instalado un sistema de control por vigilancia, sin que haya que especificar, más allá de la mera vigilancia, la finalidad exacta que se le ha asignado a ese control. Lo importante será determinar si el dato obtenido se ha utilizado para la finalidad de control de la relación laboral o para una finalidad ajena al cumplimiento del contrato […] si la finalidad del tratamiento no guarda relación directa con el mantenimiento, desarrollo o control de la relación contractual el empresario estaría obligado a solicitar el consentimiento de los trabajadores afectados.*

En cuanto a la información sobre la finalidad sancionadora si se captan incumplimientos laborales de los trabajadores, según la SJS de Pamplona podrá ser considerado acto ilícito cualquier acto que sea contrario al ordenamiento y que constituya delito tipificado (robo, hurto, entre otros que pudieran ser objeto de alguna sanción de orden penal), como también lo es un acto que constituya una infracción administrativa y, por lo tanto, "*los incumplimientos de las obligaciones laborales quedan incluidos en esa noción*"(control del horario laboral).

En tercer lugar, y atendiendo al artículo 89.2 LOPDGDD, el empresario no podrá instalar sistemas de videovigilancia ni de grabación de sonidos en zonas destinadas al descanso de los trabajadores, como son los vestuarios, aseos, comedores o similares, sin excepciones.

Por último, hacer mención al tiempo que deben tenerse guardadas las grabaciones. Según el artículo 22.3 LOPDGDD, podrá ser por un período máximo de 30 días desde su captación, pudiendo conservarse más tiempo aquellas grabaciones que registren una infracción o incumplimiento de los deberes laborales de los empleados. Ahora bien, los datos obtenidos deberán ser puestos a disposición de la autoridad competente en un plazo máximo de 72 horas desde que se conociera la existencia de dichas grabaciones.

En cuanto al fallo del supuesto de hecho planteado inicialmente en la SJS Pamplona, una vez determinados todos los factores que afectan a la instalación de sistemas de videovigilancia y grabación de sonidos, el juez no se opone a tales grabaciones por lo referente al hecho que identifique la pelea ocasionada fuera de la empresa, pues según el artículo 89.1 LOPDGDD, serán válidas las imágenes obtenidas "*dentro de su marco legal y con los límites inherentes al mismo*". Pero sí aplica las consecuencias del incumplimiento del deber informativo en el tratamiento de los datos debido a la falta de información por parte de la empresa de que dichos datos podían ser tratados como finalidad sancionadora. Es por ello que la sentencia

[31]AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS [Recurso electrónico]: *Guía sobre el uso de videocámaras para seguridad y otras finalidades*, p. 21 y ss.

concluye que la prueba obtenida es nula de pleno derecho por la vulneración de un derecho fundamental que implica su ilicitud.

No obstante, finalmente el despido disciplinario se declara procedente porque se practicó otra prueba desvinculada de las grabaciones declaradas ilícitas, una prueba testifical de otro trabajador que vio los hechos y la agresión.

2.4. Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral

Se entiende por geolocalización toda tecnología que permite ubicar un dispositivo en un punto espacial a partir de la transmisión de sus coordenadas de posicionamiento[32]. Hay que tener en cuenta que hoy en día prácticamente la totalidad de los dispositivos móviles como *smartphones, tablets,* navegadores de los automóviles, etc., contienen aplicaciones de geolocalización.

Si bien en un principio la información de posicionamiento por sí misma no identifica de forma directa a una persona, sí puede hacerlo de forma indirecta, ya que basta con poner en relación el dato de posicionamiento del dispositivo con el de quién es su usuario, para que se pueda obtener una gran cantidad de información personal, como dónde se encuentra, qué sitios frecuenta, cuáles son sus gustos por los establecimientos de ocio que visita, las horas a las que accede a los mismos, etc. y esto supone un grave riesgo para la persona física, pues enturbia las barreras de la privacidad e intimidad, derechos que, como se ha mencionado, forman parte de los derechos fundamentales protegidos en la CE, concretamente en los artículos 18.1 y 18.4 CE.

Aplicados dichos mecanismos al ámbito laboral, la localización exacta del empleado durante su jornada laboral es uno de los sistemas de control laboral utilizados. Sobre todo, en puestos de trabajo desarrollados fuera del centro de trabajo (como es el caso de comerciales, vigilantes de seguridad, transportistas o conductores de ambulancias) y, cada vez con más frecuencia, se aplican a los trabajadores cuya prestación de servicios consista en el reparto de bienes a domicilio, ya que la localización por satélite, o geolocalización, a través de sistemas incorporados bien a dispositivos móviles o GPS en vehículos, permite a la empresa conocer la posición exacta del empleado y, por lo tanto, controlar los horarios y lugares prefijados en que se han ejecutado la prestación de los servicios.

Con el objetivo que los trabajadores no vean vulnerados estos derechos fundamentales en su entorno de trabajo, durante la prestación de sus servicios, la nueva LOPDGDD, regula el uso de sistemas de geolocalización con fines de control en el ámbito laboral en su artículo 90. Dicho artículo establece, en su párrafo primero, el derecho del que gozan los empresarios para tratar los datos obtenidos a través de sistemas de geolocalización, siempre que se hayan instalado para cumplir con sus funciones de control de los trabajadores atendiendo al artículo 20.3 ET.

[32] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Op. Cit.*, pp. 21 y ss.

En cambio, el párrafo segundo del mencionado precepto, hace referencia más bien a los derechos de los trabajadores que emergen al aplicar una medida de geolocalización por parte del empresario. Los regula estableciendo la obligación por parte del empresario de informar[33], con carácter previo a la instalación de la medida de control, "*de forma expresa, clara e inequívoca a los trabajadores o a los empleados públicos y, en su caso, a sus representantes, acerca de la existencia y características de estos dispositivos*", así como también tendrán la obligación de informarles del posible ejercicio que los trabajadores podrán realizar de los derechos de acceso, rectificación, limitación del tratamiento y supresión regulados en el Capítulo II del Título III de la LOPDGDD.

Cabe mencionar que a pesar de ser la geolocalización una medida más intrusiva que las grabaciones a través de sistemas de videovigilancia y grabación de sonidos (pues las imágenes y datos recabados por dichos sistemas pueden ser limitados a una zona en concreto, en cambio, con la geolocalización, aunque únicamente se registren los lugares públicos y durante su jornada laboral, se puede extraer, deducir, mucha más información, tal y como recoge Serrano Olivares[34]), falta en la regulación del artículo 90 LOPDGDD la obligación de hacer "*referencia expresa a la finalidad y alcance de la instalación de tales dispositivos en cuanto al contenido mínimo del derecho/deber de información"*, así como la imposición del límite del principio de proporcionalidad a la facultad empresarial de control.

Con el objetivo de perfilar lo regulado por la nueva LOPDGDD, así como garantizar una mayor salvaguarda de los derechos de intimidad y protección de datos de los trabajadores, es necesario examinar lo dictado por los tribunales. Para ello, se procederá a analizar la STSJ de Castilla-La Mancha 370/2015, de 31 de marzo y la SAN 13/2019, de 6 de febrero.

La STSJ de Castilla-La Mancha 370/2015 (Sala de lo Social, Sección 1ª), de 31 de marzo, trata un caso de despido disciplinario, conforme el artículo 54.2 ET y el artículo 48.c) del Convenio Colectivo Estatal de Empresas de Seguridad Privada 2012-2014, de un vigilante de seguridad que no desarrollaba las rutas asignadas, estando parado incluso durante horas, desatendiendo las tareas de vigilancia y comprometiendo la posición de la empresa empleadora frente a sus clientes.

El demandante ocupaba el puesto de vigilante de seguridad en una empresa[35] cuyas funciones consistían en vigilar durante el servicio de noche, con carácter aleatorio y sin horario establecido, una serie de instalaciones de ADIF, cliente de la empresa, concretamente de su Línea de Alta Velocidad. Para ello, la empresa contratante y demandada proporcionaba la herramienta de trabajo, el vehículo, al que "*lo equipaba con un sistema de control de flotas provisto de localizador GPS que está gestionado por el sistema NEO, y que permite realizar un seguimiento exhaustivo del vehículo que se está utilizando para la ejecución".* Sin embargo, dicho sistema de GPS se activaba en el momento en que se hacía uso del vehículo de empresa, por lo que no registraba ningún lugar fuera de la jornada laboral y, cabe mencionar que los trabajadores de la empresa habían sido informados de tal medida.

[33] Ver anexo 4. Consentimiento para el tratamiento de datos de geolocalización.

[34] SERRANO OLIVARES, R.; Los derechos digitales en el ámbito laboral: Comentario de urgencia a la ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales, p. 225.

[35] Eulen Seguridad, S.L.U.

La empresa, tras la revisión del sistema de GPS, observa ciertas irregularidades que podrían ser calificadas como hechos muy graves, y es que cada vez que coincidían el demandante con otro trabajador para patrullar, el GPS del vehículo dejaba constancia que éste había estado parado durante el desarrollo del servicio, quedando sin proteger ni vigilar la ruta objeto de la prestación del servicio contratado, por lo que para la empresa suponía un quebranto manifiesto de la buena fe contractual, así como una desobediencia en el trabajo, junto a la presentación de una falsedad en los partes de trabajo emitidos en relación con los datos dados por el sistema GPS del vehículo que suponen una deslealtad, fraude y abuso de confianza por parte del trabajador de la empresa. Asimismo, estos hechos se agravan en relación a la normativa de Seguridad Privada y consecuencias para la empresa, por ser el demandado un vigilante de seguridad con arma, además de ocupar el cargo de representante legal de los trabajadores que, según el artículo 64 ET, quienes ostentan dicho cargo adquieren además la obligación de servir como referente al colectivo que le ha confiado su voto.

Vistos los hechos acontecidos, el Tribunal basa sus fundamentos de derecho en dos cuestiones. Por una parte, la posibilidad de uso por las empresas de sistemas de seguimiento, como puede ser el GPS, para controlar el desempeño de las funciones laborales encomendadas bajo contrato por cada uno de sus trabajadores. Y, por otra parte, los límites que el uso de estos medios de control implica en virtud de la incidencia que ello puede tener para evitar la posible vulneración del derecho fundamental a la intimidad personal del trabajador.

La primera cuestión debe tener como base la ponderación de los derechos en conflicto, ya que la exigencia informativa no puede tenerse por absoluta, sino que deben existir limitaciones por razones constitucionalmente admisibles y previstas en la ley. Tal y como establece el TC

> *El ejercicio de tales derechos únicamente admite limitaciones o sacrificios en la medida en que se desenvuelve en el seno de una organización que refleja otros derechos reconocidos constitucionalmente en los artículos 33 y 38 CE*" y viceversa "*no debe olvidarse que hemos establecido de forma invariable y constante que las facultades empresariales se encuentran limitadas por los derechos fundamentales*[36].

Por lo tanto, a los efectos del posible uso de mecanismos de vigilancia y control por geolocalización que puedan suponer una restricción de alguno de los derechos fundamentales y, en concreto del regulado en el artículo 18.4 CE, como bien se regula en la LOPDGDD, al empresario se le impone el deber de informar de manera suficiente a dichos trabajadores de su instalación, así como de la finalidad que con la misma se persigue. Pero remitiéndonos a la STC 39/2016, este tipo de información no necesita del consentimiento específico por parte del trabajador mientras la finalidad cumpla con alguno de los derechos constitucionalmente establecidos para el empresario.

Por otro lado, a parte del deber de información de la instalación de dichos dispositivos, la sentencia analizada incluye, haciendo referencia a otras sentencias (algunas ya analizadas en el apartado de instalación de sistemas de videovigilancia para el control empresarial), que el empresario, a la hora de proceder a la instalación de dispositivos de localización a los trabajadores, estas medidas de control empresarial también deberían ser justificadas según

[36] STC 98/2000, de 10 de abril del 2000.

el principio de proporcionalidad, ya que se consideran aun más intrusivas que los sistemas de videovigilancia.

En este aspecto, los datos GPS utilizados deberían única y exclusivamente ser generados por el movimiento del vehículo utilizado por el trabajador durante la jornada del trabajo y para realizar las funciones propias de su puesto de trabajo, aspecto que implica que bien el vehículo es propiedad de la empresa o bien, el activado y desactivado del dispositivo debería estar en manos del propio trabajador o, incluso, hacer uso de las nuevas tecnologías para que el dispositivo de localización sea activado en un horario concreto, el correspondiente a la jornada laboral, y desactivado durante el resto del tiempo como pueden ser días de descanso o vacaciones de cada trabajador.

Por lo que la cuestión referente a la duración del uso de la medida no es tan importante en el juicio de proporcionalidad como lo es en la instalación de sistemas de videovigilancia, ya que una duración permanente, mientras sea durante la jornada laboral, puede incluirse dentro del ejercicio del derecho de control empresarial regulado en los artículos 33 y 38 de la CE, así como en el artículo 20.3 LET.

Ahora bien, si al trabajador se le concede un permiso por el tiempo necesario y estipulado legalmente, para el cuidado de los hijos, por un día para la mudanza, entre otros, la empresa debe advertir que puede geolocalizarte y, atendiendo al artículo 20.3 y 4 LET, podrá hacerlo, pues se podrá argumentar bajo la finalidad de verificar y justificar las faltas de asistencia al trabajo, es decir, comprobar que el trabajador ha estado realizando lo que incluye el permiso y no ha hecho uso del mismo con otro objetivo, como dedicar el día al ocio. En cambio, en caso de suspensión del contrato de trabajo, debido a que, tal y como queda establecido en el artículo 45.2 LET, las obligaciones recíprocas de trabajar y remunerar el trabajo quedan exoneradas, el empresario no tendrá tal competencia de vigilancia.

Aplicando tales criterios a este supuesto de hecho, se estima el recurso de suplicación interpuesto por la representación de la empresa por lo que se declara acreditada la procedencia del despido, pues la empresa había informado previamente de la colocación de un dispositivo GPS en el vehículo de empresa que usaba para realizar su trabajo y, además, el propio actor suscribió un documento sobre el tratamiento de datos en los que prestaba su expresa conformidad, además de quedar acreditada que la conducta del actor reviste de una gravedad indudable en cuanto a la dejación de sus funcionales laborales.

Acercándonos más a la actualidad, a las emergentes plataformas digitales (como *Deliveroo, Uber Eats, Glovo*, *Uber, Cabify,* entre otras) que ya se han encontrado con conflictos en cuanto a la relación contractual que han de tener con los trabajadores que realizan la prestación de servicios de entrega de comida o productos a domicilio o en caso de *Cabify y Uber*, respecto a sus conductores, ahora se plantea otro por la aplicación de la nueva LOPDGDD en relación con la vulneración del derecho a la intimidad y protección de datos personales de los mismos que es provocada por los dispositivos de geolocalización que se les requiere que lleven encima.

Este conflicto es recogido por la Sentencia de la Audiencia Nacional 13/2019 (Sala de lo Social, Sección 1ª), de 6 de febrero, que enjuicia un conflicto colectivo contra una empresa de entrega de pizzas a domicilio[37] en el que se solicita la nulidad del denominado por la empresa

[37] Telepizza S.A.U.

“Proyecto Tracker” que añade valor a la empresa permitiendo repartir a domicilio sus productos. Se pide la nulidad de dicho proyecto debido a que supone la obligación para aquellos trabajadores que ocupen el puesto de trabajo de repartidores, de aportar a la actividad empresarial un teléfono móvil con conexión a internet de su propiedad y, a través de una aplicación informática gestionada por la empresa, se geolocaliza el dispositivo móvil y por lo tanto al trabajador, durante su jornada laboral. A su vez, se solicita la declaración de nulidad de la cláusula resolutoria incluida en los contratos por la que la empresa, ante la negativa reiterada o imposibilidad sobrevenida de aportación del teléfono móvil o bien de hacer uso de la aplicación informática de geolocalización, podrá imponer medidas disciplinarias, incluso la extinción del contrato de trabajo al amparo de lo previsto en el artículo 49.1.b) ET, por considerarlas abusivas y arbitrarias alegando la STS 4086/2015, de 21 de septiembre de 2015.

Los argumentos que justifican la aprobación del proyecto y que sirven de defensa para la empresa son los siguientes: que la finalidad del proyecto era adaptar la compañía a las nuevas tecnologías y dar un mejor servicio al cliente al mejorar el tiempo de pedidos. De esta forma, se conseguía que la gerencia del centro tenga suficiente información para organizar debidamente los pedidos pendientes de entrega a domicilio, es decir, para otorgar los pedidos a aquellos repartidores que se encuentren más cerca del cliente, así como para que por medio de la aplicación tanto los clientes como la empresa pudieran realizar un seguimiento en tiempo casi real y mediante geolocalización de la ubicación de los pedidos realizados. Además, el teléfono móvil y la aplicación solo se utilizarían durante la totalidad de la jornada y, el sistema de geolocalización no se activa hasta que al repartidor le es asignado un pedido, “*sin que exista monitorización del pedido en el centro de trabajo*”.

Otro argumento en su defensa es que la geolocalización en el trabajo viene siendo admitida por la doctrina judicial sin necesidad de negociación, al amparo del artículo 20.1 ET, siempre que la misma sea informada, supere el juicio de proporcionalidad y se traten los datos con la diligencia debida. La empresa, bajo estos requisitos, alegó que el sistema *tracker* solo pedía los datos del correo electrónico, así como el nombre y el teléfono móvil a la hora de descargar la aplicación y, para habilitar cualquier otra función como es el acceso a la cámara, se pediría el consentimiento del trabajador.

Finalmente, la empresa demandada justifica que otras empresas ofrecían sistemas de geolocalización del sistema, concretamente su principal competidor y la empresa requiere de su implantación para mantener una oferta similar. Para encajonar dichos mecanismos de control en el juicio de proporcionalidad y en el tratamiento de datos ajustado a derecho, existe un proceso automático de borrado de datos de los ficheros con las coordenadas que se ejecuta al día siguiente de la finalización del reparto y el acceso a la plataforma automática que soporta el funcionamiento del proyecto está únicamente disponible para los técnicos de la empresa, ningún tercero puede acceder a los datos allí almacenados, atendiendo a los requisitos de protección y privacidad de datos establecidos en RGPD.

Con esos hechos probados, la AN señala que el “proyecto Tracker”, tal y como había sido implementado por la empresa, vulnera el derecho a la privacidad de los trabajadores y se declara, por tanto, su nulidad. Si bien dicha medida se encuentra dentro del ejercicio legítimo del derecho constitucional a la propiedad privada (art. 33 CE) y a la libertad de empresa (art. 38 CE) por el empresario para el desarrollo de la libre organización de la empresa (como son,

entre otros, el ejercicio de control de los empleados durante la realización de sus funciones en su lugar de trabajo durante la jornada laboral, así como la oferta de un mejor servicio al cliente), dicha medida de control mediante la geolocalización no supera el juicio de proporcionalidad. Como bien se ha mencionado en el apartado anterior y alegando lo dictado por la STC 98/2000 respecto a uno de los requisitos del juicio de proporcionalidad,

> *[…] si existen otras posibilidades de satisfacer dicho interés menos agresivas y afectantes al derecho en cuestión, habrá que emplear estas últimas y no aquellas otras más agresivas y afectantes", es justamente según la Sala, el requisito que falta y lo recoge en su sexto fundamento estableciendo "La misma finalidad se podría haber obtenido con medidas que suponen una menor injerencia en los derechos fundamentales de los empleados como pudieran ser la implantación de sistemas de geolocalización en las motocicletas en las que se transportan los pedidos o las pulseras con tales dispositivos que no implican para el empleado la necesidad de aportar medios propios y lo que es más importante, ni datos de carácter personal como son el número de teléfono o la dirección de correo electrónico en la que han de recibir el código de descarga de la aplicación informática que activa el sistema.*

Por lo tanto, al ser los datos obtenidos por la geolocalización datos personales[38] y, como se ha observado, de contenido mucho más extenso que los obtenidos por los sistemas de videovigilancia, ya que se puede extraer mucha más información de la estrictamente necesaria, se debe concluir, de acuerdo con el fallo de la última sentencia analizada que establece que el hecho de cumplir con el deber de información previa, tal y como establece el artículo 90 de la LOPDGDD, no es suficiente, la medida además debe ser proporcional, es decir, justificada, idónea, necesaria y equilibrada.

Esto queda perfectamente reflejado en la sentencia, cuando el tribunal dicta que la geolocalización en el dispositivo móvil de propiedad del trabajador no es una medida equilibrada, ya que el trabajador desconocería el tratamiento de sus datos personales recabados por la empresa; es decir, si está siendo rastreado en todo momento, incluso fuera del horario laboral, para qué se usan estos datos, para un control de los pedidos por parte de los clientes o bien como seguimiento por parte de la empresa para saber si realiza la ruta más rápida y directa y poder poner sanciones disciplinarias, etc. Es por ello, que dicha medida supone una intromisión grave en la privacidad del trabajador que vulneran los derechos reconocidos en los artículos 18.1 y 4 de la CE.

2.5. Derechos digitales en la negociación colectiva

La negociación colectiva supone la posibilidad de que sujetos privados, de común acuerdo, puedan crear normas, derechos y obligaciones, que regulen las relaciones sociales y que sean igual de exigibles que lo son los mandatos de la ley. Ante esta oportunidad, la LOPDGDD, en su artículo 91, invita a que las empresas, junto con los representantes de sus trabajadores, establezcan garantías adicionales de los derechos y libertades relacionados con el tratamiento de datos personales de los trabajadores y la salvaguarda de derechos digitales en el ámbito laboral.

Francia[39] fue el primer país europeo en aplicarlo, en el 2015. El legislador francés reconoció el derecho de los trabajadores a la desconexión digital con la "Loi Travail" nº 2016-1088, de 8 de

[38] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Op. Cit.* p.21 y ss.
[39] ALEMÁN PÁEZ, F.; "*El derecho de desconexión digital*"; Universidad de Córdoba, núm.30; junio 2017, pp. 21-28.

agosto de 2016 que introduce un nuevo artículo al Código de trabajo, concretamente el artículo 2242-8, apartado 7. En éste, se reconoce el deber de negociar las modalidades de pleno ejercicio por el trabajador de su derecho a la desconexión y la puesta en marcha por la empresa de dispositivos de regulación de la utilización de los dispositivos digitales. Esta ley se caracteriza por que al final la negociación revierte en el poder directivo del empleador, por lo que, en caso de no llegar a un acuerdo, corresponde al empresario, previa consulta de los representantes de los trabajadores, aunque no vinculante, elaborar una política de actuación al respecto. En cambio, en España, a pesar de seguir la misma línea establecida por Francia, se requiere una participación de la representación legal de los trabajadores en la aprobación de una política interna sobre el uso del derecho a la desconexión digital y formación sobre los riesgos del uso de las herramientas digitales facilitadas por la empresa.

En España, hasta ahora, las empresas regulaban el uso de las herramientas digitales en la empresa y el alcance de sus correspondientes sanciones a través de acuerdos de confidencialidad o códigos telemáticos propios de cada empresa. Con la nueva LOPDGDD se instaura la posibilidad de regular tales usos y derechos mediante negociación colectiva, ya sean del empresario como del trabajador. El pionero en aplicarlo ha sido el Grupo de Empresas AXA y la Federación de Servicios de CCOO en el año 2017. Seguido de este acontecimiento, lo han introducido empresas[40] como Ikea, Telefónica y el Banco Santander que también han actualizado sus convenios colectivos.

En el caso de AXA, los derechos digitales de los trabajadores se encuentran regulados en el capítulo III sobre la organización del trabajo y nuevas tecnologías, concretamente el artículo 14 y 15 de su Convenio Colectivo vigente. El artículo 14 viene a proteger el derecho a la desconexión digital de sus trabajadores y por ello establece:

> *Consecuentemente, salvo causa de fuerza mayor o circunstancias excepcionales, AXA reconoce el derecho de los trabajadores a no responder a los mails o mensajes profesionales fuera de su horario de trabajo.*

Pero también incluye la protección de los derechos digitales de sus trabajadores por lo referente al uso que se puede hacer de las herramientas tecnológicas puestas a disposición de la empresa. Tal protección se encuentra recogida en el apartado 15 que dicta:

> *Los trabajadores deberán hacer un uso adecuado y responsable de las herramientas puestas a su disposición. La utilización excepcional de las mismas para fines personales de carácter necesario y perentorio no supondrá incumplimiento laboral. Los sistemas y equipos informáticos de la empresa son de uso exclusivamente profesional.*
>
> *El acceso a Internet se encuentra limitado a quienes, por sus responsabilidades, precisen de su utilización por el tiempo necesario de consulta.*
>
> *En el uso de correo electrónico no será posible acceder a los e-mails de otros usuarios sin su autorización, enviar e-mails de contenido ofensivo o utilizar la cuenta de correo electrónico para fines distintos de aquéllos para lo que hayan sido asignados. AXA podrá realizar excepcionalmente, cuando existan indicios de uso ilícito o abusivo por parte de un trabajador, las comprobaciones oportunas y necesarias (entre ellas, controles periódicos o realización de auditorías), en la medida de lo posible en presencia del usuario afectado y contando con un*

[40] En cuanto al ámbito internacional, destacan por empresas que han procedido a introducir medidas para limitar los correos fuera del horario laboral, Volkswagen y Mercedes Benz.

representante legal de los trabajadores. Los sistemas de control utilizados por AXA, en la medida de lo posible, deberán ser acordados con la parte social y en todo caso ser conocidos previamente por ésta.

En el caso de IKEA IBÉRICA, S.A., si analizamos el Acuerdo[41] al que se llegó con CCOO, acuerdo aprobado y ratificado por unanimidad del comité intercentros el 27 de junio de 2018, vemos que, respecto a esta materia, únicamente presenta un artículo, el 13, que solo hace alusión a la desconexión digital, de las que incluye la aplicación de mensajería instantánea "Whatsapp", así como las redes sociales.

Ambas partes coinciden en la necesidad de impulsar este derecho, por esta razón se establece que los trabajadores/as tienen derecho a no responder cualquier tipo de comunicación por cualquier canal (correo electrónico, teléfono, Whatsapp, redes sociales, etc.) fuera de su horario de trabajo, salvo causa de fuerza mayor.

La comisión de seguimiento realizará una vigilancia de la implantación de esta medida.

En el caso de Telefónica, el Convenio Colectivo que se prevé que se apruebe próximamente aun está en fase de negociación con las organizaciones sindicales mayoritarias en España, UGT y CCOO. Ahora bien, según las noticias[42] publicadas en varios medios de comunicación, en dicho Convenio se incluyen cláusulas que reconocerán el derecho a la desconexión digital de sus empleados, respeto al tiempo de descanso una vez finalizada la jornada laboral y, será extensivo a todos los países donde opera la compañía.

Asimismo sucede con el Banco Santander y el Banco Sabadell, según el comunicado de CCOO[43] en la que reclama al Banco Sabadell que realice un gran acuerdo sindical que establezca los criterios para una ordenación racional del tiempo de trabajo:

CCOO trabajamos activamente para alcanzar acuerdos de desconexión en nuestro sector. Primero fue la aseguradora AXA, y ahora Banco Santander quienes han incorporado la desconexión como parte fundamental de sus acuerdos de regulación del tiempo de trabajo. Ahora le toca a Banco Sabadell.

Para aquellas empresas que aún no dispongan de un Convenio Colectivo que incorpore la regulación de la desconexión digital, así como otros derechos digitales de los trabajadores, en septiembre de 2018, la Generalitat de Catalunya aprobó la resolución TSF/2053/2018, de 4 de septiembre, por la que se dispone la inscripción y publicidad del Acuerdo Interprofesional de Catalunya para los años 2018-2020 con respecto a la Dirección General de Relaciones Laborales y Cualidad del Trabajo publicado en el Diario Oficial de la Generalitat de Catalunya.

[41] Exposición de motivos del acuerdo de IKEA IBÉRICA, S.A. con CCOO establece que las relaciones laborales de dicha empresa venían regulándose por lo dispuesto en el Convenio Colectivo de Grandes Almacenes y, se solicitó por el comité intercentros la modificación de los acuerdos en relación a la distribución de la jornada (el último de 2013), para adaptarlo a los cambios producidos en dicho Convenio y mejorar la conciliación de la vida laboral y familiar de los trabajadores.

[42] TELEFÓNICA, S.A. [Recurso electrónico]: *Telefónica reconoce el derecho a la desconexión digital de sus empleados;* 23 de noviembre de 2018, Madrid.

[43] CCOO [Recurso electrónico]: *El derecho a la desconexión digital: Fuera de la jornada laboral, ni llamadas, ni correos, ni reuniones.* CCOO servicios grupo Banco Sabadell; 3 de julio de 2018.

Dicha resolución es objeto de estudio para este trabajo ya que sirve de base[44] para futuros Convenios, especialmente el capítulo XV en el que su primer apartado regula el uso de las tecnologías de la información y la comunicación. En dicho apartado se establece lo siguiente:

2. Las organizaciones firmantes del Acuerdo Interprofesional de Cataluña, recomendamos que los convenios colectivos tengan en cuenta las siguientes normas para la correcta utilización de las herramientas de trabajo facilitadas por la empresa:

a) Las personas trabajadoras tendrán que hacer un uso adecuado y responsable de las herramientas puestas a su disposición. La empresa facilita el acceso en internet a sus trabajadores y trabajadoras para un adecuado desarrollo de sus funciones laborales. Previa autorización por parte de las empresas, y con los límites y términos que se establezcan, excepto que exista un protocolo negociado con la representación legal de las personas trabajadoras se podría hacer un uso moderado y proporcional de esta herramienta para hasta no estrictamente profesionales, si bien la navegación por Internet prohíbe expresamente: el acceso a páginas web que tengan contenidos racistas, sexuales o cualquier material que atente contra la dignidad y los principios morales; y el acceso a juegos.

b) Con carácter excepcional, y previa autorización por parte de la empresa se puede permitir la utilización del correo corporativo para el envío o recepción de correos electrónicos de naturaleza privada, en las condiciones establecidas por la empresa o en el protocolo negociado con la representación legal de las personas trabajadoras que pueda existir para regular esta materia.

c) En cuanto al uso de los teléfonos, las personas trabajadoras tendrán que hacer un uso responsable de los dispositivos móviles que la empresa ponga a su disposición para el desarrollo de su actividad profesional.

A su vez, respecto al derecho a la desconexión digital que se encuentra recogido en el mismo capítulo, se menciona la existencia de encontrar nuevos equilibrios entre la conciliación de la vida laboral y personal a pesar de las distorsiones que el desarrollo de las comunicaciones pueden provocar en el trabajo, así como los riesgos para la salud. Para ello, la resolución propone que los convenios colectivos puedan incluir la siguiente cláusula:

Las personas trabajadoras tienen el derecho, a una vez concluida su jornada laboral, que se respete el tiempo de descanso y vacaciones, así como su vida familiar y personal, hecho que comporta no atender comunicaciones telefónicas, mensajes o correos electrónicos, valorando las diferentes casuísticas y tratamientos diferenciados que puedan existir.

En el ámbito de la empresa, y de forma negociada con la representación legal de las personas trabajadoras, se podrá elaborar un protocolo que formalice este nuevo aspecto.

Asimismo, se pondrá en marcha actuaciones de comunicación y sensibilización, dirigidas a las plantillas y los mandos intermedios, y a la misma dirección de la empresa, sobre las pautas de trabajo derivadas del protocolo, y sobre el uso razonable de las comunicaciones y medios digitales.

[44] El Acuerdo Interprofesionales de Catalunya es el eje central que sostiene y desarrolla el marco catalán de relaciones sociolaborales, en tanto es el organizador e impulsor de la negociación colectiva en Catalunya, es el marco de las iniciativas sindicales.

CONCLUSIÓN

Con la exposición realizada en esta investigación, queda reflejada la transformación social que el desarrollo tecnológico ha promovido, especialmente desde la perspectiva empresarial y laboral. En este escenario, juega un papel importante la nueva normativa vigente, el Reglamento UE (RGPD), y la normativa española, la LOPDGDD, que, junto con la jurisprudencia, han dado un giro en materia de protección de datos personales, delimitando los derechos fundamentales asociados a la Era digital, ya recogidos en el artículo 18 CE y en el artículo 20 bis LET y también, estableciendo determinados límites al control empresarial, regulado en los artículos 33 y 38 de la CE, así como en el artículo 20.3 LET, pues como se ha mencionado en el trabajo, los derechos fundamentales no son absolutos, sino que su aplicación debe respetar a su vez intereses constitucionalmente relevantes como es la libertad de empresa.

Atendiendo a lo establecido por la legislación y decisiones de los distintos órganos jurisprudenciales citados, se realizará un asesoramiento para las empresas en base a los 5 derechos digitales de los trabajadores reconocidos por el título X de la LOPDGDD (arts. 87-91) con el objetivo de conseguir una correcta implementación y evitar las posibles sanciones que, como se deduce de las sentencias, pueden interponer tanto los tribunales de llegar el caso a juicio, o bien, las autoridades laborales de realizar inspecciones laborales, a causa de una nula o mala aplicación por parte de las empresas.

En cuanto a las empresas que hagan uso de sistemas digitales (ordenadores, teléfonos móviles, tabletas, correo electrónico, redes sociales), para poder controlar tales dispositivos sin poner en riesgo el derecho a la intimidad de los trabajadores, debido a que los hacen transparentes, deben cumplir los requisitos recogidos en la STEDH Barbulescu II, es decir:

- El empresario debe informar[45] con carácter previo a los trabajadores de las medidas de control que se llevarán a cabo para corroborar la correcta realización de las actividades laborales, así como su alcance y su puesta en práctica.
- El grado de intrusión y extensión de dichas medidas debe ser proporcional a la finalidad del control empresarial.
- La medida adoptada debe ser justificada, debe atender a un objetivo legítimo y necesaria, no debe existir otra medida menos intrusiva y con mayores garantías de los derechos de los trabajadores para alcanzar dicho objetivo.

El segundo derecho analizado es el derecho a la desconexión digital por el cual se busca volver a trazar la línea que separaba la vida profesional de la laboral que con las nuevas tecnologías ha ido haciéndose borrosa y ha provocado negativas consecuencias. Para que una empresa se considere que actúa diligentemente y sin vulnerar derecho alguno, debe no entorpecer el descanso de sus trabajadores, es decir, el tiempo de trabajo efectivo es aquel, establecido por contrato o convenio, durante el cual se llevan a cabo actividades laborales, independientemente del lugar en que se lleven a cabo, incluyendo los desplazamientos, todo el tiempo restante se debe considerar descanso y no cabe sanción del empresario por no atender a llamadas, correos electrónicos u otras peticiones con fines profesionales.

[45] Ver anexo 1. Circular informativa para los trabajadores.

Respecto al uso de dispositivos de videovigilancia o de grabación de sonidos en el lugar de trabajo, y de geolocalización como medidas de control empresarial, deben atender también a un juicio de proporcionalidad, esta vez establecido por la STEDH López Ribalda contra España, con tal de no atentar contra los derechos de sus trabajadores y poder ser consideradas pruebas válidas. Dicho juicio de proporcionalidad se basa en el cumplimiento de los siguientes requisitos:

- El empresario debe informar correctamente a los trabajadores de la instalación de las medidas de control empresarial, es decir, con carácter previo a su implantación que, en el caso de la aplicación de sistemas de videovigilancia es suficiente con la colocación de un distintivo informativo[46] en un lugar suficientemente visible. En él se debe incorporar a su vez el responsable del tratamiento de los datos que se puedan extraer y las consecuencias que pueden derivarse si se comete algún acto ilícito. Además, se ha de tener en cuenta que en el caso de geolocalización también debe incluirse información sobre el propósito de la implantación de la medida[47].
- La medida debe perseguir una finalidad de mantenimiento, desarrollo o control de la relación contractual, de lo contrario el empresario sí que requerirá el consentimiento de los trabajadores afectados por su instalación.
- Justificada, pues han de existir indicios razonables de la comisión de un acto ilícito que, en cuanto a la instalación de sistemas de videovigilancia o de grabación de sonidos puede dirigirse a un solo trabajador o a un puesto de trabajo en concreto en el que trabajen varios.
- Idónea, ya que la medida ha de cumplir con la finalidad de evitar o prevenir la comisión de un acto ilícito.
- Necesaria, no debe existir la posibilidad de ejercer el control empresarial mediante una medida menos gravosa.
- Equilibrada. En el caso de sistemas de videovigilancia o grabación de sonido la jurisprudencia hace alusión a la ubicación de las cámaras, que en ningún caso pueden ser zonas destinadas al descanso de los trabajadores, y duración de las grabaciones, que por lo general no pueden sobrepasar los 30 días a excepción de registrar una infracción. En cambio, en caso de implantación de sistemas de geolocalización, las decisiones de los tribunales dan más importancia no tanto a la duración del registro que puede ser permanente si la finalidad así lo requiere, sino a que dicho control se aplique únicamente durante la jornada laboral y no en tiempo de descanso.

Por último, con esta nueva regulación se pretende que todos estos derechos y posibles medidas de control sean recogidas de común acuerdo entre los empresarios y representantes de los trabajadores a través de los convenios colectivos, con el objetivo de salvaguardar los derechos digitales en el ámbito laboral, por ejemplo, el requisito informativo que se pretende alcanzar en toda aplicación de control, quedaría asegurado.

Sin embargo, uno de los problemas que se ha llegado a percibir con el análisis de varios de los convenios empresariales que incorporan la protección a derechos digitales es que, a pesar de ser pocas las empresas que hayan regulado tales derechos por vía de convenio colectivo, seguramente a casusa de la reciente regulación y debido a la habitualidad de regularlo por medio de políticas internas, aquellas empresas que sí lo han regulado, únicamente recogen el

[46] Ver anexo 3. Distintivo informativo de aviso de videovigilancia.
[47] Ver anexo 4. Consentimiento para el tratamiento de datos de geolocalización.

derecho a la desconexión digital con tal de proporcionar a los trabajadores una conciliación de la vida familiar y profesional, pero no se ha llegado a ningún acuerdo respecto a otro de los derechos mencionados. Y esto, aunque el artículo 91 LOPDGDD no impone limitación alguna al establecimiento de garantías para la salvaguarda de dichos derechos en el ámbito laboral. Para solventar la falta de regulación de tales derechos por vía colectiva, es importante hacer uso de las plantillas proporcionadas por la AEPD e incorporadas en el Anexo del trabajo, para evitar una mala información de la adopción de medidas de control empresarial por parte de las empresas a los trabajadores.

BIBLIOGRAFÍA

Artículos doctrinales

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS [Recurso electrónico]: *Guía sobre el uso de videocámaras para seguridad y otras finalidades.* [consulta: 25 de mayo de 2019]. Disponible en: <https://www.aepd.es/media/guias/guia-videovigilancia.pdf>.

ALARCÓN CAPARRÓS, V. [Recurso electrónico]: *GDPR: ¿qué necesitas saber del nuevo Reglamento Europeo de Protección de Datos?*. Blog de Signaturit, 4 de enero de 2018. [consulta: 25 de mayo de 2019]. Disponible en: <https://blog.signaturit.com/es/las-claves-sobre-el-nuevo-reglamento-europeo-de-proteccion-de-datos>.

ALEMÁN PÁEZ, F. [Recurso electrónico]: *El derecho de desconexión digital.* Universidad de Córdoba, núm.30, junio 2017. [consulta: 25 de mayo de 2019]. Disponible en: <http://portal.ugt.org/actualidad/2017/NEG_COL_NUM_31/D7.pdf>.

ANDEYRO, L. [Recurso electrónico]: *La utilización de programas de mensajería interna para uso personal de los empleados (Comentarios a la STC 241/2012, de 17 de diciembre)*. Deloitte en colaboración con CISS, grupo Wolters Kluwer, marzo 2013. [consulta: 25 de mayo de 2019]. Disponible en: <http://www.ciss.es/publico/deloitte/2013_73_a_058.pdf>.

BATUECAS CALEFRÍO, A. [Recurso electrónico]: *Intimidad personal, protección de datos personales y geolocalización.* Universidad de Salamanca, junio 2015. [consulta: 25 de mayo de 2019]. Disponible en: <file:///C:/Users/Usuario/Downloads/Dialnet-IntimidadPersonalProteccionDeDatosPersonalesYGeolo-5300038.pdf>.

BEL ANTAKI, J. *Nuevos derechos digitales de los trabajadores: las claves en cinco preguntas y respuestas*; Revista Aranzadi Doctrinal, febrero 2019.

BLASCO JOVER, C.; *Trabajadores "transparentes": la facultad fiscalitzadora del empresario vs derechos fundamentales de los empleades (I).* Revista Internacional y Comparada de Relaciones Laborales y Derecho del Empleo, Volumen 6, núm. 3, julio-septiembre de 2018.

CCOO [Recurso electrónico]: *El derecho a la desconexión digital: Fuera de la jornada laboral, ni llamadas, ni correos, ni reuniones.* CCOO servicios grupo Banco Sabadell; 3 de julio de 2018. [consulta: 25 de mayo de 2019]. Disponible en: <https://www.ccoo-servicios.es/archivos/bs/180703_desconexion_cas.pdf>.

GENERALITAT DE CATALUNYA [Recurso electrónico]: *Resolución TSF/2053/2018, de 4 de septiembre, por la que se dispone la inscripción y la publicación del Acuerdo Interprofesional de Cataluña para los años 2018-2020.* Diari Oficial de la Generalitat de Catalunya, 7 de septiembre de 2018. [consulta: 25 de mayo de 2019]. Disponible en: <https://dogc.gencat.cat/es/pdogc_canals_interns/pdogc_sumari_del_dogc/?anexos=1&language=es_ES&numDOGC=7702&seccion=0#>.

GOÑI SEIN, J.L. [Recurso electrónico]: *Nuevas tecnologías digitales, poderes empresariales y derechos de los trabajadores: análisis desde la perspectiva del Reglamento Europeo de*

Protección de Datos de 2016; abril 2017. [consulta: 25 de mayo de 2019]. Disponible en: <https://www.aadtyss.org.ar/files/documentos/296/21._Goni_Sein.pdf>.

IBERLEY [Recurso electrónico]: *Funciones y potestades de la Agencia Española de Protección de Datos (AEPD) en el RGDO y en la LOPDGDD*. Iberley, 12 de febrero de 2019. [consulta: 25 de mayo de 2019]. Disponible en: <https://www.iberley.es/temas/funciones-potestades-agencia-espanola-proteccion-datos-aepd-62849>.

LEGAL TODAY [Recurso electrónico]: *Primera sentencia sobre validez como prueba de la videovigilancia de los trabajadores tras aprobarse la LOPD.* 8 de marzo de 2019. [consulta: 25 de mayo de 2019]. Disponible en: <http://www.legaltoday.com/actualidad/noticias/primera-sentencia-sobre-validez-como-prueba-de-la-videovigilancia-de-los-trabajadores-tras-aprobarse-la-lopd>.

LÓPEZ CARBALLO, D. [Recurso electrónico]: *El impacto del RGPD en el ámbito del control laboral y la era de la innovación*; Wolters Kluwer, 25 mayo 2018. [consulta: 25 de mayo de 2019]. Disponible en: <http://dlcarballo.com/2018/05/25/el-impacto-del-rgpd-en-el-ambito-del-control-laboral-y-la-era-de-la-innovacion/>.

MIÑARRO YANINI, M.: *La Carta de derechos digitales para los trabajadores del Gupo Socialista en el Congreso: un análisis crítico ante su renovado interés*; CEF. Trabajo y Seguridad Social, núm.424, julio 2018.

MORENO GONZÁLEZ-ALLER, I. [Recurso electrónico]: *El derecho de los trabajadores a la desconexión tecnológica*, ElDerecho.com, Social. 17 de agosto de 2018. [consulta: 25 de mayo de 2019]. Disponible en: <https://elderecho.com/derecho-los-trabajadores-la-desconexion-tecnologica>.

ORTEGA PRIETO, E. Y ORTEGA FIGUEIRAL, E. [Recurso electrónico]: *La Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales: su aplicación en el ámbito laboral.* Noticias Jurídicas, enero 2019. [consulta: 25 de mayo de 2019]. Disponible en: <http://noticias.juridicas.com/conocimiento/articulos-doctrinales/13575-la-ley-organica-de-proteccion-de-datos-personales-y-garantia-de-los-derechos-digitales:-su-aplicacion-en-el-ambito-laboral/>.

PONCE RODRÍGUEZ, S. Y GARCÍA SÁNCHEZ, J. [Recurso electrónico]: *Control por parte de la empresa del correo electrónico del empleado*. ElDerecho.com, Laboral; 6 de abril de 2018. [consulta: 25 de mayo de 2019]. Disponible en: <https://elderecho.com/control-por-parte-de-la-empresa-del-correo-electronico-del-empleado>.

SERRANO OLIVARES, R. *Los derechos digitales en el ámbito laboral: Comentario de urgencia a la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales*; Universidad de Barcelona, 2018.

TELEFÓNICA, S.A. [Recurso electrónico]: *Telefónica reconoce el derecho a la desconexión digital de sus empleados;* 23 de noviembre de 2018, Madrid. [consulta: 25 de mayo de 2019]. Disponible en: <https://www.telefonica.com/es/web/sala-de-prensa/-/telefonica-reconoce-el-derecho-a-la-desconexion-digital-de-sus-empleados>.

ZAMORA, S. [Recurso electrónico]: *Desconexión digital ¿novedad o anécdota?*; Diario La Ley, nº 9363, Editorial Wolters Kluwer, 21 febrero 2019. [consulta: 25 de mayo de 2019]. Disponible en: <http://diariolaley.laley.es/document/DT0000288845/20190123/Desconexion-digital-¿novedad-o-anecdota%3F>.

ZAPATERO MARTÍN, M. [Recurso electrónico]: *El reto de la ordenación del derecho fundamental a la protección de datos de carácter personal en un universo digital*. Universidad Carlos III de Madrid, octubre 2018. [consulta: 25 de mayo de 2019]. Disponible en: <https://doi.org/10.20318/universitas.2019.4509>.

Legislación

España. Instrumento de Ratificación del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, hecho en Roma el 4 de noviembre de 1950 y enmendado por los Protocolos adicionales números 3 y 5, de 6 de mayo de 1963 y 20 de enero de 1996, respectivamente. (BOE, núm. 243, 10-10-1979, pp. 23564-23570).

España. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). (DOUE, núm. I. 119/2, 04-05-2016).

España. Constitución Española. (BOE, núm. 311, 29-12-1978).

España. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. (BOE, núm. 294, 06-12-2018, pp. 119788-119857).

España. Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil. (BOE, núm. 7, 08-01-2000).

España. Ley 36/2011, de 10 de octubre, reguladora de la jurisdicción social. (BOE, núm. 245, 11-10-2011).

España. Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores. (BOE, núm. 255, 24-10-2015).

Jurisprudencia

Sentencia del Tribunal Europeo de Derechos Humanos (Gran Sala), asunto Barbulescu contra Rumania, de 5 de septiembre de 2017 (ECLI:CE:ECHR:2017:0905JUD006149608).

Sentencia del Tribunal Europeo de Derechos Humanos (Sección 5ª), asunto Libert contra Francia, de 22 febrero de 2018 (ECLI:CE:ECHR:2018:0222JUD000058813).

Sentencia del Tribunal de Justicia de la Unión Europea (Sala 3ª), de 10 de septiembre de 2015, asunto C-266/14, asunto Federación de Servicios Privados del sindicato Comisiones Obreras y Tyco Integrated Security, S.L. (ECLI:EU:C:2015:578).

Sentencia del Tribunal Constitucional, de 10 de abril del 2000 (ECLI:ES:TC:2000:98).

Sentencia del Tribunal Constitucional, de 17 de diciembre de 2012 (ECLI:ES:TC:2012:241).

Sentencia del Tribunal Constitucional, de 7 de octubre de 2013 (ECLI:ES:TC:2013:170).

Sentencia del Tribunal Supremo (Sala de lo Social, sección 1ª), de 26 septiembre de 2007 (ECLI: ES:TS:2007:6128).

Sentencia del Tribunal Supremo (Sala de lo Social, Sección 1ª), de 8 de marzo de 2011 (ECLI: ES:TS:2011:1323).

Sentencia del Tribunal Supremo (Sala de lo Social, sección 1ª), de 13 de mayo de 2014 (recurso 1685/2013) (ECLI:ES:TS:2014:2618).

Sentencia del Tribunal Supremo (Sala de lo Social, sección 1ª), de 8 de febrero de 2018 (ECLI: ES:TS:2018:119).

Sentencia del Tribunal Supremo 21/2019 (Sala de lo Social, sección 1ª), de 15 de enero de 2019 (ECLI:ES:TS:2019:303).

Sentencia de la Audiencia Nacional 13/2019 (Sala de lo Social, Sección 1ª), de 6 de febrero de 2019 (ECLI:ES:AN:2019:136).

Sentencia del Tribunal Superior de Justicia de Castilla-La Mancha 370/2015 (Sala de lo Social, Sección 1ª) de 31 de marzo de 2015 (ECLI: ES:TSJCLM:2015:933).

Sentencia del Tribunal Superior de Justicia de Canarias (Sala de lo Social, sección 1ª), de 18 septiembre 2018 (ECLI: ES:TSJICAN:2018:870).

Sentencia del Tribunal Superior de Justicia de Catalunya 24/2019 (Sala de lo Social, Sección 1ª) de 8 de enero (ECLI: ES:TSJCAT:2019:186).

Sentencia del Juzgado de lo Social de Palma de Mallorca 74/2018 (Sala de lo Social nº 2), de 28 de febrero de 2018 (ECLI: ES:JSO:2018:835).

Sentencia del Juzgado de lo Social de Pamplona 52/2019 (Sala de lo Social, nº 3), de 18 de febrero de 2019 (ECLI: ES:JSO:2019:281).

Anexo 1. Circular informativa para los trabajadores

CIRCULAR INFORMATIVA PARA LOS TRABAJADORES

La presente circular tiene como objetivo básico la difusión de las funciones y obligaciones del personal de _____ en materia de seguridad de datos personales.

La protección se basa en el REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Estas normas protegen y garantizan las libertades y los derechos fundamentales de las personas físicas y especialmente su honor e intimidad. Con este fin se contemplan multas por parte de la Agencia de Protección de Datos de hasta 601.012,10€ en función de la calificación de la infracción cometida.

El citado RGPD tiene como objetivo primordial, entre otros, implementar las medidas de índole técnicas y organizativas necesarias para garantizar la seguridad que deben reunir tanto ficheros automatizados como en papel, los centros de tratamiento, locales, equipos, sistemas, programas y personas que intervengan en el tratamiento de los datos de carácter personal.

Para recoger todas las medidas definidas anteriormente y garantizar con lo dispuesto en el Reglamento de Seguridad, _____ ha elaborado un Documento de Seguridad y ha nombrado Responsable de Seguridad a _____. Estas medidas de seguridad son de obligado cumplimiento por todo el personal de la empresa con acceso a datos de carácter personal.

El citado Documento de Seguridad se encuentra a disposición de todo trabajador, previa solicitud al Responsable de Seguridad.

A continuación se presenta un resumen de los aspectos más relevantes:

- Recursos del sistema de información: Queda terminantemente prohibido utilizar dichos recursos a los que se tenga acceso para uso privado o para cualquier otra finalidad diferente de la del desempeño de sus funciones. Bajo ningún concepto puede revelarse información a persona alguna ajena a la empresa, sin la debida autorización.

- Los sistemas informáticos que dan acceso a los ficheros que contienen datos de carácter personal tendrán siempre este acceso restringido mediante un código de usuario y una contraseña, sin cuya introducción resulte imposible acceder a los datos protegidos.

- El código de usuario y la contraseña son absolutamente personales e intransferibles; por ello, los registros que se efectúen sobre operaciones realizadas bajo un código y contraseña se atribuirán, salvo prueba en contrario, al titular de los mismos y quedarán bajo su responsabilidad personal.

- Cada usuario es responsable de la confidencialidad de su contraseña, por lo que si advierte o sospecha que la misma ha podido ser conocida fortuita o fraudulentamente por personas no autorizadas, deberá registrarlo como incidencia y notificárselo de inmediato al Responsable de Seguridad, el cual asignará una nueva contraseña al usuario.

- Salidas de soportes: Toda salida de cualquier soporte y/o ordenador personal fuera de la organización deberá ser expresamente autorizada según el procedimiento descrito en el Documento de seguridad.

- Incidencias en materia de seguridad: El usuario que tenga conocimiento de la incidencia se responsabiliza directa y personalmente de comunicarla según las instrucciones determinadas en el Documento de Seguridad.

- Compromiso: Todos los compromisos anteriores deben mantenerse, incluso después de extinguida por cualquier causa la relación laboral con la empresa.

- Responsabilidad: El incumplimiento por el obligado, de cualquiera de las normas contenidas en el presente documento y, por ende, en el Documento de Seguridad podrá considerarse como un quebranto de la buena fe contractual. Si el incumplimiento tuviera carácter doloso, se emprenderán las acciones legales correspondientes para la debida depuración de responsabilidades.

Cualquier duda o comentario que pudiese suscitar el presente documento puede ser consultada o atendida por el Responsable de Seguridad.

En _____ , a ____de _____de 20__

Firma:

(Trabajador/a)

Anexo 2. Consentimiento para el tratamiento de datos biométricos

CONSENTIMIENTO PARA EL TRATAMIENTO DE DATOS BIOMÉTRICOS

De conformidad con lo dispuesto en el art. 9 del Reglamento (UE) 2016/679, de 27 de abril de 2016, o Reglamento General de Protección de Datos (RGPD), en lo relativo al tratamiento de categorías especiales de datos, _____ con CIF nº: _____ y domicilio a efectos de notificaciones en: _____, le informa de que recabará el/los siguiente/s dato/s biométrico/s:

❑ Huella Dactilar

❑ Reconocimiento facial para proceder a su tratamiento, en virtud de la relación de carácter laboral que vincula a ambas partes, y con la finalidad de:

❑ Realizar un control de identificación en los accesos al centro de trabajo.

❑ Llevar a cabo un control de presencia del empleado en el centro de trabajo.

Sus datos biométricos no serán transmitidos a terceros sin su consentimiento, salvo obligación legal, y serán conservados durante un período mínimo de cinco años, mientras usted no solicite su supresión.

Asimismo, se le informa de que le asisten los derechos de acceso, rectificación, supresión, oposición, limitación y portabilidad, pudiendo ejercitarlos mediante petición escrita a la dirección de _____, especificada en el primer párrafo.

En base a las consideraciones anteriormente descritas, _____ solicita su consentimiento expreso para el tratamiento de su huella dactilar y/o reconocimiento facial, para la finalidad señalada previamente.

❑ Consiento EXPRESAMENTE el tratamiento de mi/s dato/s biométrico/s (huella dactilar y/o reconocimiento facial) por parte de _____, para la finalidad expresada en este documento.

Don / Doña: _____ DNI: _____

Firma: _____

Anexo 3. Distintivo informativo de aviso de videovigilancia

ZONA VIDEOVIGILADA

RESPONSABLE:

PUEDE EJERCITAR SUS DERECHOS DE PROTECCIÓN DE DATOS ANTE:

MÁS INFORMACIÓN SOBRE EL TRATAMIENTO DE SUS DATOS PERSONALES:

Anexo 4. Consentimiento para el tratamiento de datos de geolocalización

CONSENTIMIENTO PARA EL TRATAMIENTO DE DATOS DE GEOLOCALIZACIÓN

Don/Doña:_____, con DNI nº _____
mediante el presente documento MANIFIESTA que AUTORIZA a:_____, con domicilio en: _____ y NIF/CIF nº _____, para recabar y tratar automatizadamente en un fichero del que es responsable los datos de geolocalización recogidos a través de (indicar el sistema de geolocalización) _____ , con previo consentimiento de quien firma el presente documento.

Así mismo, el firmante del presente documento, declara que ha sido previamente informado por el Responsable o Representante de _____ en lo concerniente a lo siguiente:

1. Que, _____ dispone de un fichero de Recursos Humanos, cuya finalidad es proceder a la gestión adecuada de los trabajadores y de las funciones adquiridas en _____.

2. Que los datos de carácter personal obtenidos van a ser incorporados en el fichero de Recursos Humanos.

3. Que, _____ dispone de todas las medidas de seguridad en materia de protección de datos de carácter personal recogidas en el Real Decreto 1720/2007 de 21 de diciembre.

4. Que, _____ podrá ceder a terceros los datos personales facilitados por el abajo firmante, únicamente con objeto de que se realicen determinados tratamientos para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario.

5. Que puede ejercitar, en todo momento, los derechos ARCO (Acceso, rectificación, cancelación y oposición) reconocidos en la LOPD, en los términos y condiciones que la normativa aplicable establecen, ante _____, como Responsable del Fichero en la dirección postal facilitada al inicio de este documento.

Y en prueba de conformidad, el abajo firmante da su aceptación y consentimiento para que los datos referentes a su localización geográfica sean incluidos en el fichero de Recursos Humanos.

En _____, a _____de _____ de 20____

Firma trabajador: Firma Responsable empresa: